ICANN | GNSO

通用名称支持组织

gTLD 注册数据临时规范快速政策制定流程第 2 阶段的最终报告

2020 年 7 月 31 日

本文档的来由状况

本文档是 GNSO 快速政策制定流程 (EPDP) 团队针对提交至 GNSO 理事会的《gTLD 注册数据临时规范》第 2 阶段提供的最终建议报告。

序言

本最终报告旨在记录 EPDP 团队的以下工作内容：(i) 对章程问题的审议结果，(ii) 收到的关于 EPDP 第 2 阶段初步报告和 EPDP 团队后续分析的意见，(iii) 政策建议和相关共识程度，以及 (iv) 实施指南，供 GNSO 理事会审议。

目录

本文档已翻译为多种语言，仅供参考之用。原始官方版本（英文版）可在以下位置找到：
https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

1 执行摘要

1.1 背景

2018 年 5 月 17 日，ICANN 董事会（以下简称“董事会”）采纳了《通用顶级域 (gTLD) 注册数据临时规范》（以下简称“临时规范”）。为了符合欧盟《通用数据保护条例》(“GDPR”)，“临时规范”修改了《注册服务机构认证协议》和《注册管理机构协议》中的现行要求。[1]根据《ICANN 章程》，“临时规范”将于 2019 年 5 月 25 日过期。

2018 年 7 月 19 日，GNSO 理事会启动了快速政策制定流程 (EPDP)，并授权针对“临时规范”为 gTLD 注册数据团队制定 EPDP。根据章程规定，EPDP 团队成员有明确的人数限制。但是，所有感兴趣的 ICANN 利益相关方团体、选区和支持组织均可派遣代表参与 EPDP 团队。

在第 1 阶段的工作中，EPDP 团队的任务是，确定是将《gTLD 注册数据临时规范》一字不改地纳入“ICANN 共识性政策”，还是适当修改后再纳入。本最终报告是关于 EPDP 团队章程所规定的第 2 阶段工作，具体包括：(i) 就非公开注册数据的标准化访问/披露系统进行讨论，(ii)《gTLD 注册数据临时规范》附录中指出的问题（即，“社群后续行动中的重要问题”），以及 (iii) 第 1 阶段悬而未决的问题，例如，法人与自然人，城市字段修订等。有关更多详情，请参阅此处。

为顺利组织开展工作，EPDP 团队同意将其工作分为第 1 优先级议题和第 2 优先级议题进行处理。第 1 优先级议题由 SSAD 以及与 SSAD 直接相关的各类问题构成。第 2 优先级议题包括以下主题：

- 信息显示：附属和认证隐私/代理提供商
- 法人和自然人
- 城市字段编辑
- 数据留存
- ICANN 首席技术官办公室 (OCTO) 的潜在职责
- 为特殊联系人设置统一匿名电子邮件的可行性
- WHOIS 准确度报告系统的准确度

[1] 可从 https://eur-lex.europa.eu/eli/reg/2016/679/oj 获取 GDPR；有关 GDPR 的信息，请参阅 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/。

EPDP 团队一致认为，应优先完成第 1 优先级事项的审议工作。但也普遍赞同，如果可行，团队还将同步处理第 2 优先级事项并尽力取得进展。

1.2 初步报告和初步报告附录

2020 年 2 月 7 日，EPDP 团队发布了初步报告以征询公众意见。初步报告概括了讨论的非公开 gTLD 注册数据的标准化访问/披露系统（简称“SSAD”）提案及随附初步建议的相关核心问题。

2020 年 3 月 26 日，EPDP 团队发布了初步报告附录以征询公众意见。这份附录囊括了 EPDP 团队针对以上第 2 优先级事项提出的初步建议和/或结论。

在初步报告和初步报告附录发布后，EPDP 团队：(i) 继续寻求关于法律问题的指导，(ii) 认真审查公众对初步报告和附录的意见，(iii) 继续与团队成员代表的社群团队审查现行工作，以及 (iv) 继续对本最终报告的编写进行审议，并将最终报告提交给 GNSO 理事会审查，如获批准，则转发给 ICANN 董事会进行审批，如获批准，则作为 ICANN 共识性政策。按照《GNSO 工作组指南》的要求，EPDP 团队主席针对最终报告中提出的建议召开了几次共识性电话会议，详情请见附录 D。概括如下：

- 十一 (11) 项建议达成全面共识（第 1、2、3、4、11、13、15、16、17、19 和 21 项建议）
- 三 (3) 项建议达成共识（第 7、20 和 21 项建议）
- 六 (6) 项建议获得大力支持，但存在严重异议（第 5、8、9、10、12 和 18 项建议）
- 两 (2) 项建议存在分歧（第 6 和 14 项建议）

有关这些审议结果的更多详细信息，请参阅附录 D 以及 GNSO 工作组指南第 3.6 节。

GNSO 理事会审议建议（请参阅第 3 章，以了解完整的建议内容）：

SSAD 建议：

建议 #1. 认证

建议 #2. 政府实体的认证

建议 #3. 请求的标准与内容

建议 #4. 回执

建议 #5. 响应要求

建议 #6. 优先级

建议 #7. 请求者目的

建议 #8. 签约方授权

建议 #9. SSAD 处理自动化

建议 #10. 确定 SSAD 响应时间的可变 SLA

建议 #11. SSAD 条款和条件

建议 #12. 披露要求

建议 #13. 查询策略

建议 #14. 财务可持续性

建议 #15. 日志记录

建议 #16. 审计

建议 #17. 报告要求

建议 #18. 成立 GNSO 常任委员会，审核关于 SSAD 的政策建议的实施情况

第 2 优先级建议：

建议 #19. 信息显示：附属和/或认证隐私/代理提供商

建议 #20. 城市字段

建议 #21. 数据留存

建议 #22. 目的 2

第 2 优先级建议结论：

结论 1. OCTO 的职责

结论 2. WHOIS 准确度报告系统的准确度

由于外部依赖条件和时间限制，本最终报告未能涵盖所有第 2 优先级事项。具体而言，以下事项未予说明：

法人和自然人：尽管第 2 阶段针对该问题开展了一些审议工作，但未能就新的政策建议达成一致意见。流程后期收到关于此主题的研究请求，鉴于时间过于紧张，未能如期完成审议。因此，根据 EPDP 第 1 阶段建议，允许注册服务机构和注册管理运行机构对法人和自然人注册进行区分，但并未规定相关义务。GNSO 理事会正在考虑就这个问题开展进一步的工作（包括 ICANN 组织关于区分域名注册数据目录服务 (RDDS) 中的法人与自然人的研究审议工作）。”

为特殊联系人设置统一匿名电子邮件的可行性：EPDP 团队收到了法律指导意见，其中指出，发布统一屏蔽的电子邮件地址会导致个人数据公开；表明按照 GDPR 的规定，大范围发布屏蔽的电子邮件地址的方法目前或许还不可行。GNSO 理事会正在考虑就这个问题开展进一步的工作。

EPDP 团队将与 GNSO 理事会就如何解决其余的第 2 优先级事项进行磋商。

1.3 结论及后续措施

本最终报告将提交至 GNSO 理事会接受审议和审批。

1.4 本报告的其他相关章节

为了全面审核 EPDP 团队的议题及相关交流，本最终报告包括以下章节：

- 正在审议的问题的背景；
- 参与 EPDP 团队审议的人员文档（包括参与记录），以及意向声明的链接（如果适用）；
- 一份附录，包括 GNSO 理事会采纳的章程中规定的 EPDP 团队的使命；以及
- 通过正式 SO/AC 和 SG/C 渠道征集的社群意见的文档，包括响应。

2 EPDP 团队所采用的方法

本部分概括介绍 EPDP 团队采取的工作方法和思路。下述观点旨在为读者提供 EPDP 团队审议和流程的相关背景信息，不应解读为 EPDP 团队的全部工作成果和审议结果。

2.1 工作方法

EPDP 团队于 2019 年 5 月 2 日启动第 2 阶段审议工作。团队同意，除与电子邮件清单中的联系人交流意见以外，每周将安排一次或多次电话会议，继续主要通过电话会议开展工作。此外，EPDP 还召开了四次面对面会议：第一轮面对面讨论于 ICANN 第 65 届摩洛哥马拉喀什公共会议期间举行；两轮专题面对面会议（即第二次和第四次会议）分别于 2019 年 9 月和 2020 年 1 月在 ICANN 洛杉矶总部召开；第三轮面对面讨论于 ICANN 第 66 届加拿大蒙特利尔公共会议期间举行。所有 EPDP 团队会议均已记录到维基工作空间，包括电子邮件清单、草案文件、背景资料以及 ICANN 支持组织和咨询委员会（包括 GNSO 利益相关方团体和选区）提出的意见。

EPDP 团队还制定了一份工作计划，并定期审核及更新工作计划。为便于开展工作，EPDP 团队使用模板将公众对选区和利益相关方团体声明的各类请求意见制成表格（请参阅附录 D）。此模板还广泛用于记录其他 ICANN 支持组织和咨询委员会的意见，请参阅附录 D。

ICANN 第 66 届蒙特利尔公共会议期间，EPDP 团队召开社群会议，会上展示了方法和初步调查结果，供广大 ICANN 社群成员开展讨论并征询反馈意见。

2.2 思维导图、工作表和构建模块

为确保就第 2 阶段审议工作将要解决的主题达成共识，EPDP 团队使用以下思维导图绘制主题，进而对主题进行重新编组与合并（请参阅思维导图）。这为后续制定第 1 优先级和第 2 优先级工作表（请参阅工作表)奠定了基础，EPDP 团队将通过工作表采集以下信息：

- 问题描述/相关章程问题
- 预期交付成果
- 必读文献
- 即将发布的简报
- 法律问题
- 相关性
- 拟定时间安排和方法

EPDP 团队主席还提出了大量工作定义，确保 EPDP 团队审议期间的术语一致性并对所使用术语的含义达成共识（请参阅工作定义）。

在审核大量现实生活用例后，EPDP 团队建立了构成标准化访问/披露系统（简称“SSAD”）的一系列构建模块，同时认识到关于各参与方角色和责任的决议可能会受到欧洲数据保护理事会（简称“EDPB”）法律建议和指导意见的影响。

2.3 第 1 优先级议题和第 2 优先级议题

为顺利组织开展工作，EPDP 团队同意将其工作分为第 1 优先级议题和第 2 优先级议题进行处理。第 1 优先级议题由 SSAD 以及与 SSAD 直接相关的各类问题构成。第 2 优先级议题包括以下主题：

- 信息显示：附属和认证隐私/代理提供商
- 法人和自然人
- 城市字段编辑
- 数据留存
- ICANN 首席技术官办公室 (OCTO) 的潜在职责
- 为特殊联系人设置统一匿名电子邮件的可行性
- WHOIS 准确度报告系统的准确度

EPDP 团队一致认为，应优先完成第 1 优先级事项的审议工作。但也普遍赞同，如果可行，团队还将同步处理第 2 优先级事项并尽力取得进展。

由于外部依赖条件和时间限制，本最终报告未能涵盖所有第 2 优先级事项。具体而言，以下事项未予说明：

法人和自然人：尽管第 2 阶段针对该问题开展了一些审议工作，但未能就新的政策建议达成一致意见。流程后期收到关于此主题的研究请求，鉴于时间过于紧张，未能如期完成审议。因此，根据 EPDP 第 1 阶段建议，允许注册服务机构和注册管理运行机构对法人和自然人注册进行区分，但并未规定相关义务。GNSO 理事会正在考虑就这个问题开展进一步的工作（包括 ICANN 组织关于区分域名注册数据目录服务 (RDDS) 中的法人与自然人的研究审议工作）。”

为特殊联系人设置统一匿名电子邮件的可行性：EPDP 团队收到了法律指导意见，其中指出，发布统一屏蔽的电子邮件地址会导致个人数据公开；表明按照 GDPR 的规定，大范围发布屏蔽的电子邮件地址的方法目前或许还不可行。GNSO 理事会正在考虑就这个问题开展进一步的工作。

2.4 法务委员会

在认识到 EPDP 团队根据章程要求在第 2 阶段解决的很多问题的复杂性后，EPDP 团队申请面向 Bird & Bird 的外部法律顾问提供资源。为协助准备 Bird & Bird 草案法律问题，EPDP 领导层选择组建法务委员会，法务委员会由法律经验丰富的 EPDP 团队成员组成。

第 2 阶段法务委员会共同审核了 EPDP 团队成员提出的问题，以确保：

1. 问题本质上合法，但并非政策或政策实施问题；
2. 秉持中立的态度对问题进行分组，避免假定结果及选区立场；
3. 问题对于 EPDP 团队工作既贴切又及时；以及
4. 本着负责任的态度利用有限的预算聘请外部法律顾问。

法务委员会将所有约定问题问题提交到 EPDP 团队最终签署，而后再将问题发送给 Bird & Bird，但有关自动决策的问题除外。

迄今为止，EPDP 团队同意将八个 SSAD 相关问题发送给 Bird & Bird。有关问题全文及征询问题意见期间接收的法律建议执行摘要，请参阅附录 F。

2.5 章程中提出的问题

解决章程中提出的问题期间，[2]EPDP 团队对以下一些方面进行了审议：(1) 各小组在审议过程中提出的意见；(2) 第 1 阶段提出的相关意见；(3) 各小组在回应与特定章程问题相关的初步意见时提出的意见；(4) 针对工作表中的各项主题确定的必读文献；(5) 回应公众意见论坛期间提出的意见；以及 (6) EPDP 团队法律顾问 Bird & Bird 提出的意见。

[2]附录 A 进一步详细介绍了建议及章程中提出的相关问题所涉及的各项主题之间的关联。

3 EPDP 团队对章程中提出的问题和建议的回应

审查初步报告及初步报告附录公众意见后，EPDP 团队提交意见供 GNSO 理事会审议。本最终报告展示了 EPDP 团队内部针对不同建议达成的共识级别。概括如下：

- 十一 (11) 项建议达成全面共识（第 1、2、3、4、11、13、15、16、17、19 和 21 项建议）
- 三 (3) 项建议达成共识（第 7、20 和 21 项建议）
- 六 (6) 项建议获得大力支持，但存在严重异议（第 5、8、9、10、12 和 18 项建议）
- 两 (2) 项建议存在分歧（第 6 和 14 项建议）

有关这些审议结果的更多详细信息，请参阅附录 D 以及 GNSO 工作组指南第 3.6 节。

但就 SSAD 相关建议而言，EPDP 团队认定这些建议相互依存，鉴于此，GNSO 理事会必须将这些建议视为一个整体并将其呈交给 ICANN 董事会。

注：EPDP 团队工作第 1 阶段，EPDP 团队的任务是审核临时规范。临时规范是对 GDPR 做出的回应。[3]因此，GDPR 是本报告中明确引用的唯一法律。EPDP 团队一直在实施审议，判断可否独立于任何特定法律起草本最终报告，但 EPDP 团队确定明确引用法律有利于制作报告，进而促进实施团队建议。GDPR 是一项覆盖多个司法管辖区的区域法律；而且，鉴于其中包含多项严格标准，倘若遵守这项法律，则符合其他国家或适用区域数据保护法规定的概率较高。EPDP 团队完全认可 ICANN 实现全球包容性的伟大愿望，本报告中的任何内容均不应推翻基本原则：签约方有能力且必须遵守地方适用法律和法规。

3.1 非公开注册数据标准化访问/披露系统 (SSAD)

附录 A 中提供了与 EPDP 团队审核的方法和材料有关的更多详细信息，以便解决章程中提出的问题并表达以下建议。

EPDP 团队针对集中式模型和分散式模型进行了审慎考量。集中式模型是指 ICANN 或其指定处理人负责处理请求和披露授权；分散式模型是指签约方负责处理请求和披露决定。本团队无法针对任一模型达成一致意见，因而提出了一套混合式模型，即所有请求将采取集中管理模式，而披露决定（初步实施时）则将由签约方做出。混合模型 SSAD 基于以下总体原则开发而来：

[3] “本《gTLD 注册数据临时规范》（简称‘临时规范’）制定了临时要求，使 ICANN 和 gTLD 注册管理运行机构和注册服务机构能够继续遵守根据 GDPR 制定的现行 ICANN 合同要求和社群制定的政策。”

- 如果技术和商业方面可行且法律允许，必须保证签约方 SSAD 请求的接收、验证和传输实现全面自动化。披露决定（初步实施时）通常由签约方做出，而且只有在技术和商业方面可行且法律允许的情况下方可自动做出披露决定。倘若区域自动化不符合这些标准，则将实现披露决定流程标准化作为基本目标。必须依托长久以来在处理 SSAD 披露请求和响应过程中积累的丰富经验，为进一步简化和规范响应提供依据。
- 鉴于认识到需要基于体验对 SSAD 的运行状况进行调整，因此应设立 GNSO 常任委员会，负责监控 SSAD 的实施情况并提出可供采取的改进建议。通过此流程提出的改进建议不得违反 EPDP 制定的政策、数据保护法、ICANN 章程或者 GNSO 程序和指南。
- 务必制定并强制执行服务水平协议 (SLA)，但服务水平协议可能需要不断调整，因而要意识到将需绘制学习曲线。
- 披露请求响应（无论手动完成审核还是触发自动回复）均由相关签约方直接对请求者做出，但必须确立相应的日志记录机制，以便 SSAD 确认是否符合 SLA 以及是否按政策处理响应（例如，拒绝或授权披露请求时必须通知中央网关）。

本模型的优势为：

通过单一位置提交请求

- 减少请求者追踪单个联系人或遵循各项程序所花费的时间及投入的精力
- 确保将请求直接路由到各披露实体的责任方，从而消除因请求未妥善接收或落入无处理权限的实体而引发的不确定因素
- 提供明确的外展机会，宣传请求获取非公开注册数据的位置和方法
- 请求和响应可供追踪，以确定是否符合 SLA

标准化申请表

- 减少因信息不充足而遭到拒绝的披露请求数量
- 提高披露实体的请求审核效率
- 降低请求者的不确定性，而今请求者拥有一组标准/统一数据供其在提交披露请求时提供
- 降低要求披露方单独提供一组必要信息的需求

内置验证流程

- 加快披露实体审核流程，因为他们不再需要重新验证请求者
- 确认请求者经过验证的外部保证有助于提高披露几率和/或加快披露速度

标准化审核与响应流程

- 允许创建通用响应格式
- 允许制定可供披露方在审核及回复请求时遵循的规则、指南和最佳实践

- 允许采用通用响应审核系统
- 允许待定请求者自动处理某些待定请求
- 在某些情况下，促进自动披露决定
- 此外，ICANN 组织也可以通过记录请求和响应来审计披露实体行动、识别系统性违规情况及采取相应的强制措施

主要 SSAD 角色与职责：

- 中央网关管理器——由 ICANN 组织负责执行或监督的角色。负责管理要求对负责签约方进行人工审核的 SSAD 请求的受理和路由。负责根据相关政策建议制定和约定的标准，或者基于 GNSO 常任委员会针对审核 SSAD 政策建议实施情况提出的建议，管理和指导确认自动提交至签约方以发布数据的请求。负责收集有关请求、响应及做出的披露决定的数据。
- 认证当局——由 ICANN 组织负责执行或监督的角色。具备 SSAD 用户正式“认证”权限的指定管理实体，即有权确认和验证用户身份（以标识符凭证为代表）及与身份凭证相关的主张（或申诉）（以签名主张为代表）。
- 身份供应商——负责 1) 验证请求者身份和管理与请求者相关的标识符凭证；2) 验证和管理与标识符凭证相关的签名主张。在 SSAD 中，身份供应商可以是认证当局本身，或者认证当局也可以依靠零个或多个第三方执行身份供应商服务。
- 签约方——负责回复不符合自动响应标准的披露请求。[4]
- 审核 SSAD 政策建议实施情况的 GNSO 常任委员会——ICANN 社群委员会代表，负责评估因采用的 ICANN 共识性政策和/或其实施情况而产生的 SSAD 运营问题。GNSO 常任委员会的职责是审查 SSAD 运营过程中生成的数据，除根据审查现有共识性政策对 SSAD 运营的影响提出建议以外，还可以就如何最有效地对 SSAD 做出运营调整（严格实施措施）向 GNSO 理事会提出建议。

预计适用协议中将对不同的角色和职责进行详细说明和确认。

以下详细列出了 EPDP 团队提交征询社群意见的基本假设和政策建议。

3.2 ICANN 董事会和 ICANN 组织意见

为帮助提供审议依据，EPDP 团队与 ICANN 董事会和 ICANN 组织进行了沟通，“了解董事会关于其自愿代表 ICANN 组织承担的与非公开注册数据披露决策相关的运营责任范围及责任级别的立场，以及为此可能需要满足的先决条件”。

[4]默认情况下，中央网关管理器将披露请求发送至注册服务机构，但不排除在特定条件下中央网关管理器将披露请求发送给注册管理机构（请参阅建议 5 了解更多详细信息）。

ICANN 组织于 2019 年 11 月 19 日做出回复，其中有一部分指出，“ICANN 组织提议运营网关，以便传输授权数据。如上所述，网关运营商还未决定是否提供披露授权。授权提供商将参考拟定的模型确定是否满足披露标准。如果请求通过授权和认证，网关运营商将可向签约方请求数据并向请求者披露相关数据集”。[5]

ICANN 董事会于 2019 年 11 月 20 日做出回复，其中有一部分指出，“董事会一贯主张开发非公开 gTLD 注册数据访问模型。如果 EPDP 第 2 阶段团队就工作达成共识性建议，一致认为 ICANN 组织负责履行一项或多项 SSAD 运营职能，董事会将采纳这项建议，除非董事会通过超过三分之二的董事会成员投票确定该政策并不符合 ICANN 社群或 ICANN 的最佳利益。鉴于董事会主张开发访问模型并支持 ICANN 组织就拟定的 UAM 与 EDPB 进行对话，董事会可能会采纳据此提出的 EPDP 建议。

EPDP 团队向 ICANN 组织提出了大量其他澄清问题，请在以下位置查看问题和回复：https://community.icann.org/x/5BdIBg。该意见同时附上 ICANN 组织标准化访问/披露系统提案成本估算。

EPDP 团队对这项意见、比利时数据保护机构反馈及公共评议期间收到的意见进行了审议，做出最终的 SSAD 角色和职责分配决定。

3.3 SSAD 基本假设

EPDP 团队根据以下基本假设提出政策建议。这些基本假设不一定会对签约方提出新的要求；相反，假设是为了辅助最终报告读者和最终政策实施者理解 EPDP 团队提出 SSAD 模型及相关建议的意图和基本假设。

- SSAD 的目标是为非公开注册数据的访问/披露提供一种可预测、透明、有效、可问责的机制。
- SSAD 必须遵守 GDPR。
- SSAD 必须能够遵循这些衡策原则和建议。
- 鉴于 EPDP 团队已做出 SSAD 模型决策，现阶段假设将 ICANN 和签约方视为联合控制人。这项定义根据对所拟定政策的事实分析得出。

3.4 本文档的通用规范

文档中的关键字“必须”、“不得”、“要求”、“应该”、“不应”、“建议”、“不建议”、“可以”和“可选”按照 BCP 148、RFC2119 和 RFC8174 进行解释。

[5]请注意，此处描述的模型与 EPDP 团队在本报告中提出的 SSAD 模型不同。

注：注意 EPDP 团队选择的模型、等待就各方责任提出具体法律建议及确定数据控制权，因为它们适用于拟定的模型，EPDP 团队强调建议中的有些陈述可能需要从强制性改为宽松性，有些陈述则可能需要从宽松性改为强制性。（例如，“必须”改为“可以”等等）。

在引用实施指南的位置，EPDP 团队会考虑提供补充信息和/或澄清信息，帮助提供政策建议实施依据，但 EPDP 团队指出实施指南的重要性和地位与政策制定建议内容有所不同。

3.5 EPDP 团队 SSAD 建议

3.5.1.定义

- **认证**——认证当局声明用户有资格在部署一系列规定保护措施的特定安全配置下使用 SSAD 所采取的管理行动。
- **认证当局**——具备 SSAD 用户正式“认证”权限的指定管理实体，即有权确认和验证用户身份（以标识符凭证为代表）及与身份凭证相关的主张（或申诉）（以签名主张为代表）。
- **认证当局审计师**——负责履行认证当局审计要求的实体，请参阅建议 16（审计）。此类实体可以是独立机构；如果 ICANN 组织最终将认证当局角色外包给第三方，则 ICANN 组织也可以作为认证当局审计师。
- **验证(Authentication)**——验证请求者身份凭证和签名主张的过程或行动。
- **授权**——批准或者拒绝披露非公开注册数据的过程。
- **中央网关管理器 (CGM)**——由 ICANN 组织负责执行或监督的角色。 负责管理要求对负责签约方进行人工审核的 SSAD 请求的受理和路由。负责根据相关政策建议制定和约定的标准，或者基于 GNSO 常任委员会针对审核 SSAD 政策建议实施情况提出的建议，管理和指导确认自动提交至签约方以发布数据的请求。负责收集有关请求、响应及做出的披露决定的数据。
- **取消认证当局的认证资格**——ICANN 组织撤消与认证当局的协议所采取的管理行动；如果将此职能外包给第三方，则此后不得继续作为认证当局运行。
- **符合资格的政府实体**：为在职权范围内履行公共政策使命而访问非公开注册数据的政府实体（包括本地政府和国际政府间组织）。
- **身份凭证**：简洁表示标识符与验证信息之间的关联性的数据对象，可用于验证实体尝试访问系统时所声称的身份。示例：用户名/密码、OpenID 凭证、X.509 公开密钥证书。
- **身份供应商**——负责 1) 验证请求者身份和管理与请求者相关的标识符凭证；以及 2) 验证和管理与标识符凭证相关的签名主张。在 SSAD 中，身份供

应商可以是认证当局本身，或者认证当局也可以依靠零个或多个第三方执行身份供应商服务。

- **请求者**——请求通过 SSAD 披露域名注册数据的授权用户。
- **撤消用户凭证**——身份供应商声明先前的有效凭据失效的事件。
- **签名主张**：简洁表示标识符凭证与一项或多项访问主张之间的关联性的数据对象，可用于验证实体尝试执行有关访问所提出的主张。示例：[Oauth 凭证]、X.509 属性证书。签名主张可以特定于用户（例如，指示专业组织协会或确认合法数据处理流程），也可以特定于请求（例如，指示披露请求的合法依据）。
- **非公开 gTLD 注册数据标准化访问/披露系统** (SSAD)——SSAD 是指构成请求、验证和披露系统的整套当事团体和组成部分。
- **核实(Validate/validation)**——测试、证明或核实结构的健全性或正确性。（示例：在授权过程中，披露者将核实身份凭证和签名主张）。
- **验证（Verify，动词）**——测试或证明事实或值的真实性或准确性。（示例：身份供应商先验证请求者身份再颁发身份凭证。）
- **验证（Verification，名词）**——通过检查信息确定声称事实或值的真实性或准确性的过程。

3.5.2.建议

建议 #1. 认证[6]

1.1. EPDP 团队建议成立或选择认证当局。

1.2. EPDP 团队建议认证当局根据以下建议制定政策，以便对 SSAD 用户进行认证。

1.3. 以下建议必须纳入认证政策：

1.3.1. SSAD 必须仅接受认证组织或个人提出的访问/披露请求。但是，认证请求必须充分考虑所有预期系统用户的需求，包括提出单一请求的个人或组织。重复性系统用户与一次性系统用户的认证要求可以有所不同。

1.3.2. 法人和/或个人均可获得认证。使用认证实体（例如，法人）凭证访问 SSAD 的个人保证，个人严格按照认证实体的授权行事。

1.3.3. 认证政策规范的是由 ICANN 组织管理的单一认证当局，负责验证、颁发和持续管理身份凭证和签名主张。认证当局必须出台隐私政策。认证当局可以联合外部或第三方身份供应商验证与这些请求认证相关的身份和授权信息。届时可将外部或第三方身份供应商作为

[6]注意，认证并非指代 GDPR 第 42/43 条所述的认证/证明概念。

信息交换中心。无论哪一方负责完成处理任务，始终由认证当局负责处理个人数据。如果 ICANN 组织选择外包认证当局的职能或部分职能，则 ICANN 组织将始终负责监督承接外包职能或部分职能的团体。监督必须包括监控承接外包职能或部分职能的团体面临的潜在滥用问题并解决相关问题。

1.3.4. 注册服务机构、注册管理机构或中央网关管理器（如适用）按照请求标准与内容建议（建议 3）的要求，根据身份凭证、签名主张和数据核实结果做出注册数据披露授权决定。

1.4. 认证当局要求

1.4.1. 验证请求者身份：认证当局必须验证请求者身份，进而生成身份凭证。

1.4.2. 管理签名主张：认证当局可以验证并管理一组与请求者身份凭证关联的动态主张/申诉。此验证操作可以由身份供应商完成，进而生成签名主张。签名主张[7]传达以下信息：

- 关于请求目的的主张
- 关于请求法律依据的主张
- 表示使用标识符凭证识别的用户与相关组织存在关联的主张
- 关于法律合规性（例如，数据存储、保护和留存/处置）的主张
- 关于约定出于所述正当合法目的使用披露数据的主张
- 关于遵守保护措施和/或服务条款的主张。一经发现违反保护措施和/或服务条款，则予以撤消
- 关于滥用问题预防、审计要求、争议解决、投诉流程等的主张
- 特定于请求者的主张——例如，商标所有权/注册
- 授权书声明（如适用）。

1.4.3. 除请求中包含的信息以外，必须对身份凭证和签名主张进行验证，以便决定接受还是拒绝 SSAD 请求授权。为避免存疑，单凭这些凭证不得提供自动访问/披露授权。但是，在某些合法情况下，可以自动做出访问/披露授权决定。

1.4.4. 授权当局必须制定基本“行为准则”，[8]出台一系列有助于妥善实施数据保护法（如 GDPR）的规则，包括：

- 简明扼要的解释性说明。

[7]明确声明，签名主张采用动态形式，可以根据请求（目的、法律依据、类型、紧迫性等）做出调整，而标识符凭证采用静态形式，通常不会更改。签名主张仅用于关联/捆绑属性与身份。属性根据各项请求做出动态调整，但必要时可在认证过程中进行预先审查和管理。认证当局可以预先为特定标识符凭证建立不同的主张，也可以根据每一项请求动态创建主张。具体方法将在实施阶段新一步确定。认证当局可以针对每个标识符凭证存储多个签名主张，但请求者必须根据请求调用相关主张。

[8] 为避免存疑，此处引用的行为准则并非是指 GDPR 中所述的行为准则。此处引用的行为准则是指认证当局将遵守的一系列规则和标准。

- 确定涵盖的处理操作的规定范围（SSAD 的核心是披露操作。）
- 用于监控合规性的机制。
- 指定认证当局审计师（即监控机构），定义支持该机构履行职能的机制。
- 描述与利益相关方开展“协商”的程度。

1.4.5. 认证当局必须出台隐私政策，以处理负责的个人数据及认证用户服务条款，请参阅建议 11。

1.4.6. 建立基本申请程序：认证当局必须面向全体身份供应商（如适用）和申请认证的全体申请人建立统一基本申请程序和附带要求，包括：

i. 认证时间表
ii. 定义认证用户资格要求
iii. 身份验证和程序
iv. 身份凭证管理政策：生命周期/到期日期、续约频率、安全属性（密码或密钥策略/强度）等
v. 身份凭证撤消程序：撤消条件、撤消机制等（另请参阅下方的“认证用户撤消和滥用”部分）
vi. 签名主张管理：生命周期/到期日期、续约频率等
vii. 注意：某些类别的请求者的要求可能需要超出上述基本标准。

1.4.7. 制定争议解决和投诉流程：认证当局必须制定争议解决和投诉流程，对认证当局采取的行动提出质疑。制定的流程必须包含正当流程监督制衡机制。

1.4.8. 审计：认证当局必须定期接受审计师审计。一经发现认证当局违反认证政策和要求，将提供机会纠正违规行为；但是，如果一再违反政策和要求，则必须寻找或成立新的认证当局。此外，必须定期对认证实体进行审计，确定其是否遵守认证政策和要求（注意：有关认证当局及其可以采用的任何身份供应商的审计要求的详细信息，请参阅审计建议 16。）

1.4.9. 用户组：认证当局可以划定用户组/类别以简化认证流程，因为所有请求者均需通过认证，认证将包括身份验证。

1.4.10. 报告：认证当局必须定期公开报告收到的认证请求数、批准/续约的认证请求数、拒绝的认证数、撤消的认证数、收到的投诉数以及与之合作的身份供应商的信息。另请参阅建议 17 了解报告。

1.4.11. 续约：认证当局必须制定认证续约时间表并确定认证续约要求。

1.4.12. 确认用户数据：认证当局必须定期（例如，每年一次）向认证用户发送提醒，确认用户数据，并提醒认证用户保留最新认证所需的信息。如果更改上述必填信息，可能需要重新认证。

1.5. 认证用户撤消

1.5.1. 在 SSAD 中，撤消是指认证当局有权撤消认证用户的 SSAD 认证用户身份。[9] 尽管下表中所列的内容并不详尽，但在以下情况下可能会撤消资格：1) 认证用户违反适用保护措施或服务条款；2) 更改认证用户的附属组织；3) 违反数据留存/销毁要求；或者 4) 认证先决条件不再适用。

1.5.2. 认证当局必须出台申诉机制，允许认证用户在认证当局确定的特定时间段内对取消认证用户资格的决定提出质疑。但申诉期间，认证用户身份将处于暂停状态。必须采用透明方式报告申诉结果。

1.5.3. SSAD 必须出台机制，对违反保护措施或服务条款的认证用户进行举报。[10] 举报必须提交认证当局进行处理。认证当局也可以从其他团体获取信息，以确定是否存在滥用问题。

1.5.4. 个人/实体撤消政策应包括分级处罚；处罚将在实施过程中进一步细化，包括如何在其他 ICANN 领域应用分级处罚。换言之，并非每次违反系统规定都会导致撤消资格；但是，如果认证当局根据以下方法认定认证个人或实体严重违反认证条件且未能予以纠正，则可撤消资格：i) 收到经第三方查实的投诉；ii) 认证当局或审计师的审计或调查结果；iii) 误用或滥用提供的特权；iv) 屡次违反认证政策；v) DPA 审计或调查结果。

1.5.5. 如果个人/实体内部存在滥用行为模式或做法，则可根据分级制裁暂停或撤消个人或实体凭证。

1.5.6. 撤消资格必须防止此后有机构在未达到令认证当局满意的特殊条件下再次进行认证。

1.5.7. 为避免存疑，取消认证资格不妨碍个人或实体未来根据 EPDP 第 1 阶段报告建议 18（合理合法的披露请求）规定的访问方法提交请求。

1.6. 取消身份供应商授权

1.6.1. 取消身份供应商授权：身份供应商验证程序应包括分级处罚。换言之，并非每次违反政策都会导致取消授权；但是，如果根据以下方法认定身份供应商严重违反认证条件且未能予以纠正，则可取消授权：i) 收到第三方投诉；ii) 认证审计师或审计师的审计或调查结果；iii) 误用或滥用提供的特权；iv) 屡次违反认证政策。根据身份供应商取消授权的性质和条件，可以撤消部分乃至全部悬而未决的凭证或将这些凭证过渡给其他身份供应商。

[9]明确声明，不会因认证与法律实体认证关联的单个用户的单一行为而自动取消法律实体的资格，但实体可能需要对认证与法律实体认证关联的单个用户的行为负责。

[10]注意，如果认证用户存在 SSAD 滥用问题，则根据建议 13 进行处理。

1.6.2. 认证当局必须出台申诉机制，允许身份供应商对即取消身份供应商授权的决定提出质疑。但申诉期间，身份供应商身份将处于暂停状态。必须采用透明方式报告申诉结果。

1.7. 认证实体或个人的其他考虑因素：

1.7.1.必须同意：

1.7.1.1. 仅出于所述正当合法目的使用数据；
1.7.1.2. 服务条款，其中描述了合法数据使用方法；
1.7.1.3. 防止滥用收到的数据；
1.7.1.4. 在审计过程中，配合处理审计或信息请求；
1.7.1.5. 一经发现滥用数据或认证政策/要求的问题，则应取消认证资格；
1.7.1.6. 根据适用法律存储、保护和处置 gTLD 注册数据；

1.7.2. 仅出于披露要求中所述之目的的需要保留 gTLD 注册数据。

1.7.3. 特定时期内可以提交的 SSAD 请求数不设上限，除非认证实体对 SSAD 构成明显威胁，或者可能会在其他方面受到这些建议的限制（如建议 1.5(d) 和 13(b)）。据了解，SSAD 可能面临的响应能力和速度限制可能适用。

1.7.4. 必须使认证和验证所需的信息保持最新状态，并在相关信息发生更改时立即通知认证当局。任何更改都可能需要对提供的特定信息片段重新进行认证或验证。

实施指南

1.8. EPDP 团队就认证提出了以下实施指南，但同时理解实施阶段还将补充更多细节：

1.8.1. 公认的成熟适用组织可支持认证当局作为身份供应商。如上方第 1.3(f) 节所述，如果有这样信誉卓著的成熟组织与认证当局合作，必须进行适当的审查。

1.8.2. 认证当局或身份供应商可以要求认证申请人提供其他信息，包括：

- 商业登记号码及发放商业登记号码的当局名称（如果申请认证的实体是法人）。
- 商标所有权主张信息。[11]

[11] 明确声明，服务提供商和/或商标所有人代理律师也有资格获得认证。但是，上述服务提供商和/或律师代表商标所有人行事。如果上述服务提供商和/或律师违反 SSAD 规则，则必需向披露实体提供相关数据；而且必须明确，此类违规可能会计入通过代理代表其行事的商标所有人的未来披露行为。不可通过使用其他第三方代理规避过往 SSAD 滥用制裁。

1.9. 认证当局和身份供应商审计/记录

1.9.1. 认证当局和身份供应商将记录认证/验证活动（如认证请求及做出身份认证或验证决定所依据的信息）。

1.9.2. 如果认定披露记录数据是开展以下工作的必要条件，仅应通过认证当局或身份供应商披露记录数据或以其他方式供其评审：a) 履行认证当局或身份供应商的适用法律义务；b) 根据本政策实施审计；或者 c) 支持 SSAD 和认证政策合理运转。

另请参阅审计和记录建议了解更多详细信息。

1.10. 验证。ICANN 组织应发挥自身在其他涉及验证问题的领域（如注册服务机构认证）的丰富经验，提出在实施阶段验证请求者身份的提案。

1.11. 重新认证期。作为最佳实践，可以考虑重新认证期和注册服务机构要求，目前为 5 年。为避免存疑，任何行为均不能阻止认证当局在认证续约时要求提供补充文件。

1.12. 预计认证实体将制定适当的政策和程序，以确保个人适当使用凭证。每位用户均必须经过认证，但代表组织行事的用户必须将个人认证与组织认证进行关联。

建议 #2. 政府实体的认证

2.1. 认证目标

对于因完成公共政策任务而需要访问注册数据的实体，SSAD 必须提供合理的注册数据访问权限。考虑到适用数据保护规则下规定的各项义务，负责处理构成个人数据的注册数据的控制人将在授予非公开注册数据访问权限方面享有最终决策权。

制定和实施政府实体专用认证程序，有助于签约方在向特定实体授予非公开注册数据访问权限或自动处理中央网关管理器做出的披露决定（如适用）之前做出必要决定。这项认证程序可以为数据控制人提供必要信息，以便评估数据披露行为并做出披露决定。

2.2. 注册资格

国家/地区政府机构或其授权机构认证[12] 适用于需要访问非公开注册数据以完成公共政策任务的各种合格政府实体[13]，包括但不限于：

- 民事和刑事执法机构
- 数据保护和监管机构
- 司法机关
- 依法或受政府实体委托处理公共政策任务的消费者权益组织
- 依法或受政府实体委托处理公共政策任务的网络安全机构，包括计算机紧急事件响应小组 (CERT)

2.3. 资格审查

合格政府实体是指需要依据适用数据保护法访问非公开注册数据以完成公共政策任务的实体。实体是否符合资格由国家/地区指定的认证当局决定。此项资格审查不影响签约方决定是否在请求非公开注册数据后披露个人数据的最终决策权，也不影响中央网关管理器在请求满足披露决定自动处理（如适用）标准情况下的决策权。

2.4. 政府认证当局的要求

政府认证要求必须遵守建议 1.3 中规定的要求。

此外，必须列出要求并将要求提供给合格政府实体。如果未能遵循这些要求，可能导致 ICANN 组织取消认证当局的认证资格。

2.5. 认证程序

认证必须由经认可的认证当局提供。该认证当局
可以是国家/地区政府机构（例如，部门），也可以委托给国际政府间组织。认证当局应发布认证要求，并对合格政府实体执行认证程序。

2.5.1. 认证重点强调数据请求者（接收者）的责任，数据请求者负责遵守法律。
2.5.2. 认证侧重满足法律要求，如数据留存时间、安全存储、组织数据控制和违规通知要求。
2.5.3. 续约、记录、审计、申诉和取消认证事宜将根据建议 1 进行处理。

[12]实施注意事项：此类机构可以是国际政府组织。
[13]国际政府间组织 (IGO) 同样符合建议 2 的认证资格要求。如果 IGO 希望获得认证，必须通过主办国家/地区的认证当局进行认证。

实施指南：

2.6. 如果政府实体要加入 SSAD，需通过认证。未经授权的政府实体可以在 SSAD 之外提出数据请求，且签约方应制定程序以规范提供合理的访问权限。
2.7. 一旦经过认证，用户需遵守政策提出的保护建议（另请参阅建议 11“SSAD 条款和条件”）。这并不影响实体遵守国内法律规定的保护措施。
2.8. 认证实体应提供详细信息，辅助对签约方做出披露决定，如与请求相关的任何适用当地法律。

建议 #3. 请求的标准与内容

3.1. 这项建议的目标在于采用标准化方法提交请求的数据元素，包括任何支持文件。

3.2. EPDP 团队建议，每项 SSAD 请求必须包含披露决定所需的全部信息，包括以下信息：

3.2.1. 与访问/披露请求有关的域名；
3.2.2. 标识请求者信息，包括建议 1 第 1.4a) 节和第 1.4b) 节定义的身份和签名主张信息；[14]
3.2.3. 关于请求者在请求方面具有的特定法律权限、合法权益、其他法律依据和/或请求理由（例如，合法权益或其他法律依据是什么？为何请求者需要请求此数据？）；
3.2.4. 确认本着善意的原则提出请求，仅出于 (c) 中规定的目的依法处理接收的数据（如果有）；
3.2.5. 请求者请求的数据元素列表，以及为何请求的数据元素是实现请求目的的必要条件；
3.2.6. 请求类型（例如，紧急性——另请参阅建议 6“优先级”；机密性——另请参阅建议 12“披露要求”）。

3.3. 中央网关管理器[15]必须确认提供所有必要信息。如果中央网关管理器检测到请求不完整，中央网关管理器必须向请求者指出请求不完整，详细说明缺少哪些必要数据，并为请求者提供完善请求的机会。请求者不得提交不完整的请求。

[14]加入 SSAD 的各方均需充分考量可能适用于跨境数据传输的各项要求。
[15]请参阅第 3.5.1 节“定义”部分的定义。

实施指南

EPDP 团队希望：

3.4. 每项请求必须包括与上方第 3.2 节所述的信息相关的数据。虽然这项政策未指定收集数据并将数据纳入请求的机制（无论网络表格、API 还是类似格式），但应考虑提供预先填充的字段、复选框和/或下拉选项。尽管如此，使用预先填充的字段、复选框或下拉选项时，不得妨碍请求者行使提交自由格式响应的权利。

3.5. 除非接收请求的签约方表示同样愿意使用其他语言接收请求和/或支持文件，否则必须使用英语提交请求。

3.6. 签名主张可以提供上方列出的一项或多项要求。

建议 #4. 回执和披露请求转发

4.1. 回执

4.1.1. 在确认请求语法正确并已填写所有必填字段后，中央网关管理器必须立即同步做出回复，发送回执并将披露请求[16] 转发给负责相关事务的签约方。

4.1.2. 另外，中央网关管理器在回复请求者时还应提供后续步骤信息、获取公开注册数据的方法信息以及符合建议 10 中所述的 SLA 的预期时间表。

4.2. 披露请求转发

4.2.1. 默认情况下，中央网关管理器必须将披露请求转发给记录的注册服务机构。但是，如果中央网关管理器意识到根据这些建议开展评估时需要向相关注册管理运行机构提出披露请求，则中央网关管理器可以将披露请求转发给相关注册管理运行机构，但必需向注册管理运行机构提供传输请求的原因供其参考。请求者必须能够在中央网关管理器中标记此类情况，但中央网关管理器必须自行评估标识的情况，确定是否需要向相关注册管理运行机构提出披露请求。明确声明，这项建议中的任何内容均不妨碍请求者在 SSAD 之外直接与相关注册管理运行机构联系并提出披露请求。

实施指南

EPDP 团队希望：

4.3. 回执将包括“通知单号”或类似机制，以促进请求者与 SSAD 互动，具体细节将在实施阶段确定。

4.4. 中央网关管理器将披露请求及所需的适当请求者信息转发给签约方。如果涉及适用于披露决定自动处理机制的披露请求（请参阅建议“自动化”），则可在中央网关管理器指示签约方将请求的数据自动披露给请求者时转发披露请求及所有相关信息。

建议 #5. 响应要求

5.1. 对于中央网关管理器：[17]

5.1.1. 在转发给负责相关事务的签约方的过程中，中央网关管理器可向签约方提出建议以决定是否披露。

5.2. 对于签约方：

5.2.1. 签约方可以遵循中央网关管理器的建议，但并未规定相关义务。如果签约方决定拒绝遵循中央网关管理器的建议，则签约方必须提供不遵循中央网关管理器建议的原因，以便中央网关管理器汲取教训并完善未来响应建议。

5.2.2. 除非遇到特殊情况，否则必须及时做出披露响应，不得无故延误。上述特殊情况可能包括收到的请求总数远远超过 SLA 规定的情形。[18] 符合自动响应标准的 SSAD 请求必定收到自动披露响应。倘若请求不符合自动响应标准，则必须根据 SLA 建议中所述的 SLA 接收响应。

5.2.3. 如果拒绝披露（全部或部分）数据，必须在响应中提供足以使请求者客观理解做出拒绝决定的理由，例如分析和解读平衡测试应用方法[19]（如适用）。此外，签约方还可以在响应中包含关于如何获取公开注册数据的信息。

5.2.4. 如果签约方确定披露违反适用法律或导致违背相关政策建议，则签约方必须记录理由并将此信息传输给请求者，如果需要，还应告知 ICANN 组织。

5.3. 如果请求者认为请求遭拒违反本政策的程序要求，可以向 ICANN 组织提起申诉。ICANN 组织必须根据其执行流程调查披露请求申诉。

[17]注意，建议 9 中介绍了符合自动披露决策标准的披露请求要求。

[18]有关哪些行为视为滥用 SSAD 的更多详细信息，请参阅建议 12。

[19] 根据建议 6，必须采取谨慎态度，避免在本说明中向请求者披露任何个人数据。

5.4. ICANN 组织必须出台警报机制，如果请求者及被披露数据的数据主体认为披露或非披露是签约方系统性滥用行为的后果，则可运用该机制向 ICANN 组织发出警报。该警报机制不属于申诉机制——并非用于通过法院或数据保护机构一类的可用争议解决机制对披露或非披露相关方提出质疑——而是帮助向 ICANN 合规部通报有关系统性违反本政策要求的指控，因此应触发相应的强制措施。

实施指南

5.5. 警报机制生成的信息同样有望纳入 SSAD 实施状态报告（请参阅建议 18），以便进一步审议处理滥用行为的潜在补救措施。

5.6. EPDP 团队并不希望中央网关管理器从第一天起就开始提出建议，因为据了解中央网关管理器需要先积累经验，才能向签约方提出相关建议。预计将自动提出建议，充分考量请求中包含的信息、请求者相关信息及请求者的请求历史记录。

建议 #6. 优先级

6.1. EPDP 团队建议中央网关管理器至少提供以下三 (3) 个优先级，以便请求者通过 SSAD 提交请求时做出选择。优先级定义签约方就披露请求采取行动的紧迫性：

6.1.1. **第 1 优先级**——紧急请求——确定紧急请求的标准仅限于可能威胁生命、严重人身伤害、破坏重要基础设施（在线或离线）或儿童剥削等的情况。为避免存疑，第 1 优先级不仅限于执法机构要求。

6.1.2. **第 2 优先级**——ICANN 行政诉讼程序——此类披露请求是根据 ICANN 合同要求或现有共识性政策（如 UDRP 和 URS 验证请求）提起行政诉讼程序得出的结果。[20]

6.1.3. **第 3 优先级**——所有其他请求。

6.2. 对于第 3 优先级请求，请求者必须能够指出披露请求涉及消费者保护问题（网络钓鱼、恶意软件或欺诈）；在这种情况下，签约方会暂时搁置其他第 3 优先级请求而优先处理此类请求。持续滥用该指示可能会导致请求者被取消认证资格。

[20]明确声明，在 ICANN 行政诉讼程序中，预计将仅限对 ICANN 批准的争议解决服务提供商或其员工分配优先级。

6.3. 签约方：

- 可以在请求审核期间重新指定优先级。例如，手动审核请求时，签约方可能会发现，尽管将优先级设置为第 2 优先级（ICANN 行政诉讼程序），但请求并未提供任何证明 ICANN 行政诉讼程序的证据，如提交的 UDRP 案例，因此应将请求重新归类为第 3 优先级。
- 必须将重新归类传达给中央网关管理器和请求者。

6.4. EPDP 团队建议，SSAD 必须支持“紧急”SSAD 披露要求，届时将适用以下要求：

6.4.1. 滥用紧急请求：违反紧急 SSAD 请求使用规则将导致中央网关管理器做出响应，以确保事先了解并满足紧急 SSAD 请求要求，然而一再违反使用规则可能导致中央网关管理器暂停通过 SSAD 提出紧急请求的功能。

6.4.2. 如果 SSAD 请求已标记为“紧急”，签约方必须指定专用联系人处理紧急 SSAD 请求，届时将可以通过中央网关管理器存储和使用紧急 SSAD 请求。

6.5. EPDP 团队建议，签约方必须在 SSAD 门户中发布标准工作时间、工作日和相应时区。

实施指南

6.6 请查看注册管理运行机构应对安全威胁的框架以供参考，其中指出：“*初步就可以评估为‘高优先级’的请求应该是十分明显的问题，不需要特别的技能就能确定它是影响到公共安全的威胁。‘高优先级’是指报告的情况对人们的生活或重要基础设施产生直接威胁，或者涉及到剥削儿童的情况。*”

6.7 关键基础设施是指至关重要的物理和网络系统，因为一旦此类物理和网络系统功能丧失或遭到破坏，将对人身安全、经济保障、公共卫生或安全产生重大不利影响。

6.8 另请参阅建议 10，其中包含有关紧急 SSAD 请求要求的更多详细信息。

如何定义优先级？

优先级是指分配给披露请求的代码，假定将根据约定的最佳目标响应时间进行处理。

谁负责确定优先级？
披露请求的初始优先级由请求者使用本政策定义的优先级选项设置。一旦选定优先级，中央网关管理器将明确声明紧急请求适用标准及滥用此优先级设置的潜在后果。

如果需要调整优先级，会发生什么情况？
审核请求期间，可能需要重新指定初始设置的优先级。例如，手动审核请求时，签约方可能会发现，尽管将优先级设置为 2 (UDRP/URS)，但请求并未提供任何证据，如提交的 UDRP 案例，因此应将请求重新归类为第 3 优先级。无论进行任何重新归类，必须传达给中央网关管理器和请求者。收到中央网关管理器发出的非自动披露请求后，再由签约方负责确定是否披露非公开数据。在上方定义的响应时间内，签约方必须对请求做出响应。

建议 #7. 请求者目的

7.1. EPDP 团队建议：

7.1.1. 请求者必须出于特定目的提交数据披露请求，包括但不限于：(i) 刑事执法、国家或公共安全；(ii) 非执法调查和民事索赔，包括知识产权侵权及 UDRP 和 URS 索赔；(iii) 消费者保护、防止滥用和网络安全，以及 (iv) 适用于受监管实体的义务。[21]如果请求者已获得注册域名持有人 (RNH) 的同意（由请求者全权决定），则请求者还可以提交数据验证请求，例如验证 RNH 的域名注册所有权主张或与请求者签署的合同。

7.1.2. 主张其中某一个特定目的并不能保证在所有情况下都可以访问，而是取决于以下几方面的评估结果：特定请求的价值、是否符合所有适用政策要求，以及请求的法律依据。

建议 #8. 签约方授权。

明确声明，本建议与路由到签约方接受审核的披露要求有关。这些要求不适用于符合建议 9 中所述的自动处理披露决定标准的披露请求，无论是强制还是应签约方的要求自动处理披露决定。本建议不涵盖签约方根据建议 16（摘自 EPDP 第 1 阶段）从地理层面区分注册人的能力，也不涵盖签约方根据这项具体建议的建议 17（摘自 EPDP 第 1 阶段）区分法人与自然人的能力。

[21]例如，欧盟网络和信息系统安全指令（称为 NIS 指令）针对数字服务提供商和基本服务运营商提出了具体义务。

一般要求

签约方

8.1. 无论自动完成审核还是实施有效审核，必须单独（而非批量）审核每一项请求，而且不得单纯根据认证用户类别披露数据。

8.2. 可以将授权责任外包给第三方提供商，但始终由签约方最终负责确保满足适用要求。

8.3. 必须确定与披露决定相关的处理的法律依据。[22] 请求者将有权确定签约方披露请求数据预计遵循的法律依据；但是，无论在任何情况下，只要签约方负责做出披露决定，必须由签约方最终判定适当的法律依据。

8.4. 必须支持通过 SSAD 系统接收的复议请求，必须根据请求者提供的理由审议这些请求。明确声明，重新提交与原始请求相同的披露请求但未提供为何必须复议请求的支持理由，则签约方无需进行复议。

8.5. 除非有相反的法律要求，否则不得单纯因缺少以下任一条件而拒绝披露：(i) 法院指令；(ii) 传票；(iii) 待决民事诉讼；或者 (iv) UDRP 或 URS 程序；也不得单纯因请求基于声称的知识产权侵权提出这一事实拒绝披露。

授权裁决要求

收到中央网关管理器的请求后，签约方：

8.6. 必须对请求有效性实施初步审核[23]，即请求是否足以作为签约方开展实质性审核的依据及处理相关基础数据。如果签约方确定请求无效，例如未提供足够的基础数据实质性审核依据，签约方必须要求请求者在拒绝请求之前提供进一步的信息；

8.7. 如果经初步审核确定请求有效，必须对请求和基础数据开展实质性审核：

8.7.1. 如果在评估基础数据后，经签约方合理认定披露请求的数据元素不会导致披露个人数据，除非适用法律禁止披露数据，否则签约方必须披露数据。[24] 明确声明，如果披露不会导致披露个人数据，则签约方不必进一步评估请求。

[22] 另请参阅实施指南 17。

[23] 根据剑桥词典的释义，是指首次审核（根据第一次看到或听到的事实进行审核）。

[24] 如果考虑发布法人的非公开数据，特别是关于 NGO 和团体从事可能受当地法律（例如，宪法和特许权利法）保护的人权活动数据时，签约方应考虑对因披露法人数据可能被识别身份的个人产生的影响。

8.7.2. 如果在评估基础数据后，签约方认定披露请求的数据元素会导致披露个人数据，则签约方必须至少在对请求和基础数据进行实质性审核的过程中确定：

8.7.2.1. 签约方披露数据是否具有法律依据；[25]
8.7.2.2. 是否请求的所有数据元素都是必需元素；[26]
8.7.2.3. 是否根据签约方在第 8.3 节提出的法律依据的要求进行平衡或审核。

8.8. 如果请求受第 8.7.2.3 款平衡或审核规定约束：

8.8.1. 如果根据评估结果，签约方认定数据主体的权益或基本权利和自由并未超越请求者的合法利益，则必须披露数据。签约方必须记录批准理由。

8.8.2. 如果根据评估结果，签约方认定数据主体的权益或基本权利和自由超越请求者的合法利益，则必须拒绝请求。签约方必须记录拒绝理由，必须将拒绝理由传达至中央网关管理器，且务必确保拒绝理由不含任何个人数据。

8.9. 如果请求不受第 8.7.2.3 款平衡或审核规定约束：

8.9.1. 如果签约方确定披露数据具备法律依据或适用法律未禁止披露数据，则必须披露。签约方必须记录批准理由。

8.9.2. 如果签约方确定披露数据不具备法律依据或适用法律禁止披露数据，则必须拒绝请求。签约方必须记录拒绝理由，必须将拒绝理由传达至中央网关管理器，且务必确保拒绝理由不含任何个人数据。

请求者：

8.10. 如果认为请求遭到不当拒绝，可以提出复议请求。

8.11. 必须在复议请求中提供支持理由，说明为何必须复议请求。支持理由应提供足够详细的信息，说明请求者为何认为请求遭到不当拒绝。

8.12. 如果请求者认为签约方未遵守本政策的任何要求，请求者应向 ICANN 组织进一步通报建议 5“响应要求”中所述的警报机制。

[25] 另请参阅实施指南 17
[26] 如需进一步了解“必需”定义，请参阅 EPDP 团队在阐述此定义时所参考的法律指导意见第 7 页

实施指南

8.13. EPDP 团队设想签约方能够通过 SSAD 中的专用通知单与请求者进行通信。另外，EPDP 团队设想根据适用数据保护法和网络安全措施，通过行业标准数据保护技术（包括加密技术）保障个人数据传输安全，为 SSAD 提供充分保护。

8.14. EPDP 团队指出如何在政策实施阶段评估第 8.6 款规定的沟通细节；但是，EPDP 团队会提供额外指导加以辅助。EPDP 团队设想签约方将通过相关 SSAD 通知单向请求者发送通知，声明拒绝请求的决定。接着，请求者将有 (x) 天时间向签约方提供更新信息。请求者提供更新信息时，SLA 响应时间将重置。例如，签约方将有 1 个工作日对更新后的紧急请求做出响应。如果请求者选择不提供信息，则签约方向请求者发送“拒绝意向”通知时会计算 SLA。如果请求者决定不做出响应，则规定时间段结束后，请求将被拒绝。

8.15. 当签约方评估请求者的合法利益时，签约方应考虑以下几个方面：

8.15.1. 权益必须具体、真实、顺应当前局势，而不模糊、单凭臆测判断。

8.15.2. 只要遵守数据保护法及其他法律，则通常视为利益合法。

8.15.3. 合法权益包括：(i) 法律主张执行、行使或辩护，包括知识产权侵权；(ii) 防止欺诈和滥用服务；(iii) 物理、IT 和网络安全。

8.16. 在实质性审核中，签约方至少应评估：

8.16.1.应根据以下元素（如适用）确定是否保证数据主体的权益或基本权利和自由未超越请求者的合法利益。任何一项元素均无法解决结果；相反，签约方应从整体角度综合考虑以下情形：

8.16.1.1. *影响评估*。考量对数据主体的直接影响及处理数据可能产生的更广泛的后果。考量请求者为维护 DNS 的安全和稳定而追求的公共利益和合法利益。每当披露请求的条件或要披露的数据性质暗示相关数据主体面临的风险增加时，做出决策时均应考量到这一点。

8.16.1.2. *数据性质*。考量数据的敏感度及数据是否已公开可用。

8.16.1.3. *数据主体身份*。考量数据主体的身份是否会导致其面临的风险进一步增加（例如，儿童、寻求庇护者、其他受保护群体）

8.16.1.4. *处理范围*。考量披露请求或其他相关情况的信息，有人提出是否需要妥善保护数据（低风险），而不是公开披露数据、

允许大量人员访问数据或与其他数据合并（高风险），[27] 但这并不是为了禁止公开披露法律诉讼和管理争议解决程序（如 UDRP 和 URS）。

8.16.1.5. *对数据主体的合理期望。*考量数据主题是否合理期望以这种方式处理/披露数据。

8.16.1.6. *控制人和数据主体身份。*考量协商能力及控制人与数据主体之间是否存在权力失衡。[28]

8.16.1.7. *涉及的法律框架。*考量请求者、一个或多个签约方、数据主体的司法框架，以及可能会对潜在披露产生的影响。

8.16.1.8. *跨境数据传输。*考量可能适用于跨境数据传输的要求。

8.17. 法律依据可能取决于 ICANN 政策（或适用法律）是否提供法律依据。

应酌情修订平衡测试应用方法及本部分考量的各项元素，重点突出解读 GDPR 的适用判例法、EDPB 出台的指导原则或者未来可能对 GDPR 或其他适用隐私法做出的修订。

建议 #9. SSAD 处理自动化

9.1. EPDP 团队建议，在技术和商业方面可行且法律允许的情况下，中央网关管理器必须保证相关签约方 SSAD 请求的接收、验证和传输实现自动化。

9.2. SSAD 必须允许自动处理来自认证用户的格式正确、完整有效且正确识别的请求，如下所述。

自动处理披露决定

9.3. 对于经确定（请参阅第 9.4 节和建议 18 所述的流程）自动化在技术和商业方面[29] 可行[30] 且法律允许的请求类别，签约方必须自动处理披露决定。为避免存疑，EPDP 团队建议，哪怕任何一类披露决定目前达不到这些标准，也不妨碍未来根据建议 18 中所述的流程将其列入自动披露范畴。倘若披露决定不符合这些标准，则将实现披露决定流程标准化作为基本目标。

[27]如需进一步了解“合并数据会增加风险”，请参阅 EPDP 团队在考量这些元素时所参考的法律指导意见第 5 页。

[28]在签约方授权背景下，相关方是指签约方（控制人）和注册人（数据主体）；但是，双方的角色和责任将在实施阶段进一步讨论。

[29]实施期间，需进一步考量注册服务机构的商业可行性（为此，收到的满足披露决定自动处理标准的请求数可能十分有限），并考量自动处理披露请求的经济负担是否达到可能需要豁免的程度。在考量过程中，中央网关管理器还应考察如何促进签约方系统与 SSAD 集成，以减轻自动处理披露决定的潜在负担。

[30] 自动处理披露决定经济可行性的初步审议工作将由 ICANN 组织联合实施审核小组共同完成，后续审议根据 SSAD 演进机制（如适用）开展。

9.4. 根据获得的法律指导意见（请参阅关于在披露非公开注册人数据的背景下恢复用例自动化的建议——2020 年 4 月），EPDP 团队建议自 SSAD 启动之日起，在 GDPR 法律允许的范围内全面自动处理以下几类披露请求（采集和处理披露决定）。

9.4.1. 来自当地或其他适用司法管辖区执法机构且满足以下要求的请求：1) 提供经证实的 GDPR 6(1)e 法律依据；或者 2) 根据 GDPR 第 2 条“豁免”条款进行处理；

9.4.2. 对涉嫌由 ICANN/影响注册人的签约方开展的违反数据保护立法的行为实施调查；

9.4.3. 仅限城市字段的请求，评估究竟是为了索赔还是出于统计目的；

9.4.4. 签约方先前未在注册记录中披露的个人数据。

9.5. 明确声明，如果签约方确定法律不允许自动处理本建议中规定的用例披露决定或通过建议 18 所述的流程处理披露决定，或者面临 EPDP 团队获得的法律指导意见未发现的重大风险，但随后通过数据保护影响评估 (DPIA) 识别并记录，签约方必须向 ICANN 组织发出通知，表明需要在自动处理所识别用例的披露决定时接受豁免，而且必须在通知中附上支持文件。不合理的豁免通知可能需要接受 ICANN 的审核。如果 ICANN 组织发现签约方通知不正确或遭到滥用，则必须撤消豁免资格。

9.6. 在通知 ICANN 组织后，鉴于需要自动处理，中央网关管理器必须停止传输识别的用例，同时必须根据建议 8“签约方授权”的要求传送请求。

9.7. ICANN 组织必须出台通知和意见征询流程，以便受影响的利益相关方就第 9.5 款提出的豁免规定发表意见。 ICANN 组织可以促进受影响的利益相关方与相关签约方之间开展后续讨论，彼此增进对豁免和支持信息的理解。实施阶段将进一步确定细节，包括流程的潜在保密事宜。

9.8. 一旦签约方意识到豁免不再适用，必须向 ICANN 组织发出相应通知。

9.9. 签约方根据第 9.8 款发出通知后，中央网关管理器必须参考本建议将符合自动处理标准的请求传输给签约方，同时签约方必须恢复对相关用例披露决定的自动处理。

9.10. 至于将要发送给签约方接受审核的披露请求，在签约方权衡风险并评估法律许可性（如适用）之后，签约方可以请求中央网关自动处理全部或某些特定类型的披露请求和/或来自特定请求者的披露决定。[31]

9.11. 签约方可以随时撤消或修订自动处理不符合这些政策建议要求的披露决定的请求。

9.12. 明确声明，中央网关管理器负责监督披露请求是否符合披露决定自动处理标准，其中可能包括通过中央网关实施非自动审核。同样，中央网关可以请求签约方提供进一步的信息，从而帮助中央网关管理器确定是否符合披露决定自动处理标准。如果需要，签约方可以提供进一步的信息。在应此类请求提供信息时不得传输任何个人数据。

实施指南

除建议 4（回执）和建议 10 (SLA)（这两项建议同样适用于自动处理披露决定）所述的要求以外，以下实施指南也适用于自动处理披露决定，即请求中央网关管理器需要根据本建议自动决定是否要从签约方获取披露要求。

9.13. EPDP 团队预计，SSAD 的各个操作环节（如请求接收、凭证核查、请求提交验证（格式和完整性，而非内容）均可实现自动化，但不可能在所有情况下自动处理披露请求审核和披露涉及的各项操作。

9.14. 在新一步考量建议 18 中规定的法律允许的潜在用例时，如果缺乏权威指南（例如，EDPB、欧洲法院 (ECJ)、新法律）指导，预计将由承担自动处理披露决定责任的一方（或多方）判定法律是否允许。

9.15. 除上述法律指导意见以外，EPDP 团队建议 GNSO 常任委员会（请参阅建议 18）在审核期间进一步考量关于在披露非公开注册人数据的背景下恢复用例自动化的建议（2020 年 4 月）附录 2 介绍的保护措施及建议第 3.4 节提出的用例，以考量披露是否存在法律影响或可能妨碍自动披露的类似重大影响。

9.16. 下面这种披露决定自动处理方法有望实现实际应用：中央网关管理器确认请求符合自动处理要求，而后指示签约方向请求者自动披露请求的数据。该机制有望在实施阶段最终确定。

[31]例如，签约方可以考虑实施可信通知方案，向满足相关签约方确立的特定标准的请求者颁发资格认证，允许对其披露请求自动做出响应。

9.17. 加入 SSAD 的各方均需充分考量可能适用于跨境数据传输的各项要求。

建议 #10. 确定 SSAD 响应时间的可变 SLA

10.1. EPDP 团队建议，签约方必须符合下方提供的实施指南，遵守建议 18 制定、实施、执行及不时更新的服务水平协议 (SLA)。

10.2. 为计算 SLA 响应时间，EPDP 团队建议中央网关管理器在向签约方提供通过验证的请求及各类支持信息时开始运行 SLA，在签约方通过中央网关做出响应并发出请求的信息、拒绝响应或其他信息请求时停止运行 SLA。为完成 SLA 计算，复议请求或请求者在响应中提供更多信息将视为发起新的请求。

非自动披露请求优先级矩阵

请求类型	优先级	拟定的 SLA[32] （合规期限：6 个月/12 个月/18 个月）
紧急请求	1	1 个工作日，不超过 3 个日历日 (85%/90%/95%)
ICANN 行政诉讼程序	2	最多 2 个工作日 (85%/90%/95%)
所有其他请求*	3	请参阅下方的实施指南。

*注意: 这些政策建议的任何规定均未明令禁止提出新类别及制定 SLA。

实施指南

10.3. 第 1 优先级和第 2 优先级要求的目的在于遵守共识性政策文件。第 3 优先级服务水平要求也可以在与 IRT 协商后列入共识性政策文件。

拟议定义

工作日：[33] 请参阅签约方所在司法管辖区的定义。
平均响应时间：所有响应时间的滚动平均值，频繁（例如，每天或每周）自动计算，是签约方随时评估自身性能的一种实用指标。
响应目标评估时间间隔：期限为 3 个月，每年可以审核 4 次响应时间性能。
响应目标值：响应目标评估时间间隔结束日的平均响应时间测量值。
合规目标值：与响应目标值的定义相同，但对此 SLA 目标进行了合规审核。

[32] 注意，表中引用的工作日自签约方收到来自中央网关管理器的披露请求之日起开始计算。
[33] 另请参阅建议 6.5。

SSAD 请求的签约方响应时间要求将分两阶段逐渐上升：

- 第 1 阶段自 SSAD 政策生效日期后**六 (6) 个月**开始。
- 第 2 阶段自 SSAD 政策生效日期后**一 (1) 年**开始。

第 1 阶段（仅适用于第 3 优先级请求）

10.4. 第 1 阶段乃至后续各个阶段，SSAD 第 3 优先级请求的签约方响应目标始终为五 (5) 个工作日。

10.5. 中央网关管理器必须使用平均响应时间衡量响应目标，而不是分别基于每一次响应进行衡量。

10.6. SSAD 必须根据签约方的持续平均响应时间计算滚动平均值，作为签约方随时评估自身性能的实用指标。

10.7. 同时，SSAD 还必须在响应目标评估间隔结束时测量持续滚动平均值的响应目标值。必须仅使用 3 个月的响应目标值确定是否达到响应目标，如下所述。为避免存疑，SSAD 之所以向签约方提供平均响应时间，其目的在于向签约方发出警告，表明响应时间可能存在问题，以便配合签约方对相关问题进行补救。因此，签约方必须有权随时查看当前响应目标值。哪怕签约方的响应目标值超过五 (5) 个工作日，也不一定会被判定为违反政策。

相反，如果未能达到响应目标，将提示 ICANN 向签约方发出警报，提醒签约方未达到响应目标。

10.8. 签约方必须在五 (5) 个工作日内就 ICANN 发出的未达到响应目标通知做出回应。

10.9. 签约方回应必须提供理由，说明为何签约方无法达到响应目标。

10.10. 如果签约方未能对 ICANN 通知做出回应，则必定视作违反政策；因此，若未对合规通知做出回应，将发起 ICANN 合规性调查。

第 2 阶段（仅适用于第 3 优先级请求）

10.11. 第 2 阶段，SSAD 第 3 优先级请求的签约方合规目标为十 (10) 个工作日。

10.12. 中央网关管理器必须使用平均响应时间衡量合规目标，而不是分别基于每一次响应进行衡量。SSAD 将于响应目标评估时间间隔的最后一天计算签约方的平均合规目标。

10.13. 如果签约方的响应目标值超过十个工作日，将导致违反政策；因此，签约方将受到合规部门的制裁。

10.14. 第一年必须至少每六个月审核一次响应目标和合规目标，而后每年审核一次（取决于第一次审核的结果）。

10.15. 如果披露请求的响应目标符合全自动响应标准，则有望在实施阶段得到进一步优化，预计将达到 60 秒以内。

10.16. 如果签约方请求提供其他信息并且请求者提供相应信息，实施审核小组应进一步考量 SLA 的影响。（请参阅建议 8“签约方授权”，以了解更多相关信息。）

建议 #11. SSAD 条款和条件

11.1. EPDP 团队建议实施阶段进一步定义相应协议和政策（如 SSAD 使用条款、SSAD 隐私政策、披露协议和可接受的使用策略）的最低期望，而后通过 SSAD 责任实体（ICANN 组织或受 ICANN 组织委托行使这项执法职能的第三方）制定并执行。这些协议和政策必须充分考量该政策提出的所有建议。预计 SSAD 各参与方将酌情制定并协商这些协议和政策，充分考量以下实施指南。

11.2. 与通过 SSAD 处理数据请求相关的所有必要协议均必须包含跨境数据传输条款，确保各方做出承诺（如适用），保证并提供充分的数据保护。

11.3. ICANN 组织可以酌情更新 SSAD 条款和条件，以满足适用法律和惯例要求。

实施指南：

11.4. SSAD 处理 SSAD 用户（SSAD 请求者和签约方）个人数据的隐私政策

EPDP 建议，隐私政策必须至少包含相关数据保护原则，包括：

- 处理的个人数据类型
- 如何及为何处理个人数据，例如，
    - 验证身份
    - 发送服务通知
- 个人数据留存时间
- 共享个人数据的第三方类型
- 由此引发的任何国际数据传输/要求的详细信息（如适用）
- 关于数据主体权利及数据主体行使这些权利的方法的信息

- 关于如何传达隐私政策更改的通知
- 透明度要求
- 数据安全要求
- 问责措施（隐私设计，默认指超过一定规模的数据保护主管 (DPO) 等）

11.5. SSAD 用户（SSAD 请求者和签约方）使用条款

EPDP 建议，使用条款必须至少列明以下信息：

- 请求者根据以下原则对控制人（负责做出披露决定的实体）进行赔偿：
  - 如果因以下情况引发第三方索赔损害或损失，则由请求者负责做出赔偿：(i) 在认证或请求过程中存在失实陈述；或者 (ii) 因误用请求的数据导致违反适用使用条款或适用法律。
  - 这些条款中的任何规定均不限制任何当事方行使适用法律赋予的责任或追偿权（即，如果法律赋予追偿权，则不排除请求者向控制人追回损失）。
  - 这些条款中的任何规定均不得解释为向不具备签署赔偿条款的合法权力的公共权威机构请求者施加赔偿义务。此外，本条款中的任何规定均不得改变政府作为 SSAD 运营商追索对象的潜在既有责任。
- 数据请求要求
- 记录和审计要求
- 合规证明能力
- 适用禁令
- 滥用问题预防要求

11.6. SSAD 请求者披露协议

EPDP 建议，向请求者披露数据后，披露协议必须至少满足对请求者提出的以下要求：

- 使用数据实现请求中指定的目的
- 使用数据实现请求中未指定的新目的时的要求
- 数据的保留与销毁：请求者必须确认，将根据适用法律存储、保护和处置 gTLD 注册数据。请求者必须仅出于实现披露请求所述之目的的需要保留 gTLD 注册数据，除非适用法律要求延长相关数据留存期。
- 合法使用数据

11.7. SSAD 请求者可接受的使用策略。请求者必须接受可接受的使用策略，才能通过 SSAD 提交披露请求。

可接受的使用策略必须至少包括以下要求：

请求者：

11.7.1. 必须仅向当前 RDS 数据集（无历史数据）请求数据；
11.7.2. 对于每一项 RDS 数据请求，必须陈述相应的处理目的和法律依据，陈述需接受审计（请参阅审计建议 16 了解更多详细信息）；
11.7.3. 可以出于多种目的分别发出请求向 SSAD 请求数据，获取同一组请求数据；
11.7.4. 对于每一项明确目的，必须提供：(i) 关于请求数据预期用途的陈述，以及 (ii) 请求者将仅出于所述之目的处理数据的陈述。这些陈述将需接受审计（请参阅审计建议 16 了解更多详细信息）。

建议 #12. 披露要求

12.1. EPDP 团队建议：

签约方：

12.1.1. 必须仅披露请求者请求的数据；
12.1.2. 必须返回当前数据或其子集（无历史数据）；

12.2. 签约方和中央网关管理器：

12.2.1.必须根据适用法律处理数据；
12.2.2. 应适用法律要求，必须根据合理请求向注册域名持有人（数据主体）披露数据，确认处理与其有关的个人数据；但请注意，法律调查或程序性质可能要求 SSAD 和/或披露实体对数据主体的某些请求保密。可以与请求实体合作，根据适用法律规定的数据主体权利，向数据主体披露机密请求；
12.2.3. 应适用法律要求，必须出台机制供数据主体行使擦除或反对自动处理个人信息的权利（如果此类处理存在法律影响或类似重大影响）及任何其他适用权利；
12.2.4. 必须使用简明扼要的语言，利用简洁透明、通俗易懂且易于访问的形式，向数据主体通报可能处理其数据的实体/第三方类型。为避免存疑，签约方必须向注册人客户发出上述通知，SSAD 必须向 SSAD 用户发出上述通知。对于签约方，此通知必须包含非公开注册数据潜在接收者的信息，包括但不限于建议 7“请求者目的”列出的接收者（如果法律允许）。此外，可能需要履行适用法律规定的信息义务，但必须至少包含上述信息。

实施指南

12.3. 当前数据是指签约方决定是否披露数据时审核的数据。为降低披露请求未决期间更改数据的概率（例如，注册人更新联系信息），强烈建议签约方在做出披露决定后尽快披露数据。为避免存疑，历史数据是指发出披露请求之前已存在的注册数据，而不是因注册人在审核披露请求到决定是否披露注册请求期间做出更新而可能更改的注册数据。

12.4. 法律调查或程序的性质不限于刑事调查或其他调查（例如，很多民事调查需要保密）。

建议 #13. 查询策略

13.1. EPDP 团队建议中央网关管理器：

13.1.1. 必须监控系统并采取适当措施，[34]如撤销或限制访问权限，防止系统滥用或误用；

13.1.2. 如果证明请求存在滥用性质，可以采取措施限制同一请求者提交的请求数量；

SSAD“滥用”可能包括（但不限于）检测出以下一种或多种行为/实践：

13.1.2.1. 大量自动提交格式错误或不完整的请求。

13.1.2.2. 大量[35]自动重复提交琐碎无聊、恶意或无理取闹的请求。

13.1.2.3. 使用错误、被盗或伪造的凭证访问系统。

13.1.2.4. 存储/延迟和发送大量请求导致 SSAD 或其他团体无法履行 SLA。根据此类特定行为调查滥用问题时，应充分考量比例概念。

13.1.3. 与其他违反访问政策的行为一样，滥用行为最终将导致暂停或终止 SSAD 访问权限。如果中央网关管理器基于滥用问题决定限制请求者发出的请求数量，但请求者认为决定不合理，可以通过 ICANN 组织进行补救。[36]为避免存疑，如果 SSAD 收到来自同一请求者的大量请求，单凭请求数量不能作为存在系统滥用问题的事实证据。

[34] EPDP 团队预计将在实施阶段进一步对“适当措施”进行定义。

[35]EPDP 团队预计将在实施阶段进一步对“大量”进行定义。

[36]明确声明，将以中央网关管理器复议的形式进行补救，请求者可以据此提供新信息，但并非强制要求。

13.1.4. 无论自动完成审议还是实施有效审核，必须仅对请求披露非公开注册数据的特定域名请求做出响应，必须单独（而非批量）审查[37]每一项请求。

13.2. EPDP 团队建议签约方：

13.2.1. 如果中央网关管理器根据上方 a) 和 b) 条款未发现滥用，则不得以滥用行为作为依据拒绝从 SSAD 披露请求。但是，签约方还必须通过某种方式将此行为汇报至 CGM/SSAD。中央网关管理器必须出台机制，供签约方报告发现的滥用请求者/请求，并在为签约方做出响应预留的时间内做出与请求者/请求相关的决定。或者，允许签约方延迟做出响应，直至中央网关管理器审核滥用报告并做出决定为止。

13.3. EPDP 团队建议：

13.3.1. 中央网关管理器必须支持键入完全合格域名（不含通配符）的请求。

13.3.2. 中央网关管理器必须支持请求者在单个请求中提交多个域名。[38]

13.3.3. 如果披露请求不支持自动处理披露决定，中央网关管理器必须将每个域名单独路由至负责做出披露决定的签约方（为此，可能要求 SSAD 将请求拆分为多项事务）。

13.3.4. 尽管提出了滥用行为管理建议，中央网关管理器和签约方必须能够根据建立的 SLA 处理合理数量的请求。

13.3.5. 中央网关管理器必须仅支持请求当前数据（不含域名注册历史记录
数据）。

13.3.6. SSAD 必须能够保存不同披露请求历史记录，以便持续跟踪 SSAD 请求者与签约方通过 SSAD 进行的交流。需要采取适当的保护措施保护此类信息。如认为有必要，应向 CP 提供对此类相关活动统计信息的适当访问权限，以确保在做出此类披露决定时充分考量与披露请求有关的所有相关信息。

另请参阅建议 11“条款和条件”中可接受的使用策略要求。

实施指南

[37]预计自动完成这项审查。

[38] EPDP 团队期望实施阶段合理确定一次性可以提交的请求数，与查询策略一致。

13.4. 滥用行为可能最终导致暂停或终止 SSAD 访问权限；但是，实施期间应考虑采用分级处罚方案。但在某些严重滥用（如伪造或窃取凭证）情况下，将立即终止访问权限。

13.5. 凡请求披露非公开注册的域名注册，必须分别针对每一个域名注册发出 SSAD 请求，但请求者必须能够同时提交多项请求，例如，通过在同一申请表中输入多个域名注册实现，但需保证适用相同的请求信息。

13.6. 关于第 13.3 节规定“如认为有必要，应向 CP 提供对此类相关活动统计信息的适当访问权限”，预计仅限适用于 CP 自身活动。

建议 #14. 财务可持续性

14.1. EPDP 团队建议，在考量 SSAD 的费用和财务可持续性时，需要区分“系统开发和运营”与“系统后续运行”。

14.2. 目标在于确保 SSAD 自负盈亏，避免额外向注册人收费。不得由数据主体承担向第三方披露数据的费用；SSAD 数据请求者应主要承担系统维护费用。此外，不得由数据主体承担处理数据披露请求的费用，签约方已在评估 SSAD 用户提交的请求后拒绝承担相关费用。ICANN 可以（部分）承担中央网关维护费用。明确声明，EPDP 团队明白，究其根本，注册人是 ICANN 的主要收入来源。这项收入本身并不违反“不得由数据主体承担向第三方披露数据的费用”的限制。 中央网关不得因第三方请求数据或向第三方披露数据而另行收费。但 EPDP 团队发现，注册域名持有人将始终间接承担注册服务机构和注册管理机构产生的各项费用。EPDP 团队还了解到，RAA 禁止 ICANN 限制注册服务机构可能出台的收费项目。RAA 3.7.12 指出：“本《协议》并未对‘注册服务机构’向注册域名持有人收取的注册域名注册费金额进行规定或限制。”

14.3. 我们将在设置 SSAD 使用费时向 SSAD 潜在用户（根据认证流程实施情况和将要使用的身份供应商确定）征询意见。特别是，哪怕潜在 SSAD 请求者并非隶属于 ICANN 社群，也必须有机会发表意见并与 IRT 进行交流。此类意见应有助于 IRT 就此主题进行审议。

14.4. SSAD 不应被视作 ICANN 或签约方的盈利平台。SSAD 基金应足以担负费用，包括分包商公平市值及建立法律风险基金。[39] 务必确保在 SSAD 中支付的任何款项均投入运营成本，而不只是简单地付费购买非公开注册数据。

[39]鉴于可能面临法律不确定性且参与提供 SSAD 的各方的法律和运营风险日益加剧，建立法律风险基金是指制定适当的合法应急计划，包括但不限于适当的保险保障及任何其他足以支付潜在监管罚款或相关诉讼费的相应措施。

14.5. 关于认证框架：

14.5.1. 必须根据申请验证费用按比例向认证申请人收取不可退还的待定费用，但在某些情况下，可以为某些类型或类别的申请人免除此类费用或将费用降至零，实施阶段应进一步规范和细化。

14.5.2. 哪怕申请人遭到拒绝，也可以重新申请，只是再次申请可能需要支付申请费。

14.5.3. 费用由认证当局确定。如果认证当局外包身份供应商职能，则身份供应商可以在咨询认证当局后自行确定费用。

14.5.4. 获得认证的用户和组织必须定期更新认证。

实施指南

14.6. EPDP 团队预计，与实施其他采纳政策建议一样，初期系统开发、部署和运营费用由 ICANN 组织、[40]签约方及其他可能参与相关工作的各方共同承担。[41] 在 SSAD 运行过程中，ICANN 组织预计将考虑扩充现有机制或通过 RFP 流程降低成本，而不是从头开始构建 SSAD 及其组件。根据商业和技术可行性衡量结果，EPDP 团队预计，对于签约方而言，SSAD 的最终成本将等于或低于手动接收和审核请求的成本。

14.7. 预计后续将按照成本分担原则运行系统，因此可能需要[42] 考虑历史成本。例如，认证相关成本将由寻求获得认证的人员承担。同样，应向 SSAD 用户收费，以抵消部分 SSAD 运行成本。

14.8. 实施和运行 SSAD 时，应避免对小型运营商造成与规模不相称的高负担。

14.9. EPDP 团队认识到，SSAD 使用费可能因请求量、用户类型及其他一些潜在因素而有所不同。另外，EPDP 团队还认识到，政府可能需要遵循特定付款限制，实施阶段应充分考量相关限制。

14.10. 费用结构及续订期将在实施阶段根据上述原则确定。EPDP 团队认识到，除非了解实际成本，否则无法设置确切费用。另外，EPDP 团队还认识到，可能需要不断审核 SSAD 费用结构。

[40] 另请参阅 ICANN 组织应 EPDP 团队的要求提出的关于标准化访问/披露系统提案成本估算意见（请参阅 https://community.icann.org/x/GIIEC）

[41]明确声明，ICANN 组织将自行承担系统开发成本。签约方将自行承担成本。

[42]历史成本是指系统开发、部署和运营成本。

建议 #15. 日志记录

15.1. EPDP 团队建议，必须出台相应的日志记录程序，促进落实这些建议中提出的审计程序。日志记录要求将涉及以下几方：

- 认证当局
- 中央网关管理器
- 身份供应商
- 签约方
- 认证用户活动，如登录尝试、查询
- 做出哪些查询和披露决定

15.2. EPDP 团队建议：

15.2.1. 中央网关管理器必须记录与中央网关管理器开展交流的所有实体的所有活动（请参见下文了解更多详细信息）。

15.2.2. 日志必须包括审计在 SSAD 背景下做出的任何决定所需的各种查询和各种项目记录。

15.2.3. 日志必须保留足够长的一段时间以完成审计并解决投诉，同时充分考量与控制人投诉有关的法定限制。

15.2.4. 日志不应包含任何个人信息。如果记录的任何信息确实包含个人信息，则需采取适当的保护措施。日志可用于生成透明度报告并公开发行。（另请参阅建议 17“报告要求”）。必须对包含个人信息的记录数据予以保密。

15.2.5. 必须通过常用的[43]机读格式保存日志，并附上所有变量的清晰描述。

15.2.6. 倘若法律允许，在以下情况下必须披露相关记录数据：

- 如果有人提起滥用索赔，认知当局或争议解决方案提供商可能要求提供日志接受审查。
- 规定应将日志进一步提供给 ICANN 和审计机构。
- 依法认定为正当法律程序的实施结果，包括相关执法机构和监管机构（如适用）。

15.2.7. 可以出于以下原因披露相关记录数据：

- 为确保系统正常运行而开展的常规技术操作。

15.2.8. 相关日志应作为提供相关数据的来源。此类数据有助于请求者和签约方自行审核统计数据。

[43]明确声明，“常用”是指被很多人广为采用的格式，而不是要求所有人使用统一格式。

15.3. 至少，必须记录以下事件：

- 与身份供应商相关的日志记录[44]
- 与认证当局相关的日志记录
  - 传入认证请求详细信息
  - 认证请求处理结果。例如，颁发身份凭证或拒绝原因
  - 撤销请求详细信息
  - 指示身份凭证和签名主张通过验证的标志
  - 唯一参考编号
- 与中央网关管理器相关的日志记录
  - 与查询内容相关的信息
  - 查询处理结果，包括状态更改（例如，已接收、待处理、正在处理、已拒绝、已批准、已批准但做出更改）
  - 比率：
    - 披露和非披露；
    - 拒绝非披露所使用的各种理由；
    - CP 披露决定和非披露决定之间的差异，以及中央网关建议。
- 与签约方相关的日志记录
  - 请求响应详细信息，例如拒绝原因、批准通知和发布的数据字段。必须存储包括拒绝原因在内的披露决定。

建议 #16. 审计

16.1. EPDP 团队建议，必须出台相应的审计流程和程序，以确保妥善监控并遵循这些建议中提出的要求。

16.2. 无论开展任何审计，审计师必须对审计期间披露的专有流程和个人信息承担合理的保密义务。

更具体地来说：

认证当局审计

16.3. 如果 ICANN 将认证当局职能外包给符合资格的第三方，则必须定期对认证当局进行审计，确保符合认证建议中提出的政策要求。一经发现认证当局违反认证政策和要求，将提供机会纠正违规行为；但是，如果一再违反政策或审计要求，则必须寻找或成立新的认证当局。如果 ICANN 组织作为认证当局，则不需要对政府实体进行审计，建议 2 中对政府实体认证和审计要求做出了详细规定。

[44]实施阶段将进一步细化。

16.4. 所有认证当局审计均必须针对评估合规性的目标而设计，审计师必须合理地提前通知任何此类审计，此通知中应适当详细说明所请求的文档、数据和其他信息类别。

16.5. 在此类审计中，认证当局必须及时向审计师提供所有响应文件、数据及证明其遵守认证政策所需的其他各类信息。

16.6. 如果 ICANN 作为认证当局，预计将采用现有问责机制解决各类认证政策违规问题；注意，在这种极端情况下，将对违规期间颁发的证书进行审核。这种审核方式应在实施阶段确立并细化。

身份供应商审计

16.7. 身份供应商必须定期接受审计，确保符合认证建议中提出的政策要求。一经发现身份供应商违反认证政策和要求，将提供机会纠正违规行为；但是，如果一再违反政策或审计要求，则必须寻找新的身份供应商。

16.8. 所有身份供应商审计均必须针对评估合规性的目标而设计，审计师必须合理地提前通知任何此类审计，此通知中应适当详细说明所请求的文档、数据和其他信息类别。

16.9. 在此类审计中，身份供应商必须及时向审计师提供所有响应文件、数据及证明其遵守认证政策所需的其他各类信息。

认证实体/个人审计

16.10. 必须在实施阶段出台相应的机制，确保认证实体和个人遵循认证建议 1 和 2 中提出的政策要求。其中可能包括因查实的投诉触发的审计、随机审计或为响应自我认证或自我评估号召而开展的审计。一经发现认证实体或个人违反认证政策和要求，将提供机会纠正违规行为；但是，如果一再违反政策或审计要求，则应将有关违规行为反馈至认证当局和/或身份供应商（如适用）以采取惩戒措施。

16.11. 所有认证实体/个人审计均必须针对评估合规性的目标而设计，审计师必须合理地提前通知任何此类审计，此通知中必须适当详细说明所请求的文档、数据和其他信息类别。

16.12. 在此类审计中，认证实体/个人必须及时向审计师提供所有响应文件、数据及证明其遵守认证政策所需的其他各类信息。

建议 #17. 报告要求

17.1. EPDP 团队建议，ICANN 组织必须定期发布 SSAD 使用和运行公开报告。为避免存疑，此建议不妨碍 ICANN 组织向 SSAD 用户发布其他非公开报告。

17.2. ICANN 组织必须在运行 SSAD 后的 3 个月到 9 个月之间发布 SSAD 状态报告或公告板，而后每季度发布一次，其中至少包括以下内容：

- 接收的披露请求数量；
- 披露请求平均响应时间（按优先级分类）；
- 请求数量（按第三方目的/依据分类，如建议 4 所示）；
- 批准和拒绝的披露请求数量；
- 自动处理的披露请求数量；
- 手动处理的请求数量；
- 关于 SSAD 财务可持续性的信息；
- 最新 EDPB 指南或最新法学理论（如果有）；
- 技术或系统难题；
- 运营和系统加强机制。

实施指南：

17.3. EPDP 团队建议在实施阶段进一步考量：

- 公共报告频率——经认定，每季度发布一次公开报告较为合理；
- 待报告的数据，预计将包括以下信息：a) 披露请求数量；b) 每一类请求者的披露请求数量；c) 每一位请求者的披露请求数量（针对法人实体）；授权/拒绝的披露请求数量；响应时间。请注意，上面列举的内容并不详尽。
- 公开报告机制——考量发布公开公告板的可能性，代替（或补充）发布的报告；
- 在某些情况下可能需要保密，如关于自然人和 LEA 请求的信息。可以考虑发布汇总数据或采用匿名化机制，以解决可能面临的保密问题。

建议 #18. 成立 GNSO 常任委员会，审核关于 SSAD 的政策建议的实施情况

18.1. EPDP 团队建议，GNSO 理事会必须成立 GNSO 常任委员会，评估因采纳 ICANN 共识性政策和/或实施政策而引发的 SSAD 运营问题。GNSO 常任委员会的职责是审查 SSAD 运营过程中生成的数据，除根据审查现有共识性政策对 SSAD 运营的影响提出建议以外，还可以就如何最有效地对 SSAD 做出运营调整（严格实施措施）向 GNSO 理事会提出建议。

18.2. 另外，EPDP 团队建议 GNSO 理事会采用以下原则并要求 GNSO 常任委员会以此为基准履行使命，必须在章程中体现这项规定：

18.2.1 构成：GNSO 常任委员会不仅应包含 ICANN 咨询委员会代表，还应包含加入当前 EPDP 团队并参与制定《gTLD 注册数据临时规范》的 GNSO 利益相关方团体和选区。GNSO 常任委员会成员应至少包含一名 GAC、ALAC、SSAC、RySG、RrSG、NCSG、IPC、BC 和 ISPCP 成员，同时上述团体至少各派遣一名候补人员。注意，团体成员数量不应影响共识流程，因为届时将以团体（而不是单个成员）为单位统计立场。GNSO 理事会也可以考虑邀请 ICANN 组织联络人加入 GNSO 常任委员会。

18.2.2. 职责范围：章程必须由 GNSO 理事会与咨询委员会（例如，GAC、SSAC 和 GNSO 常任委员会 ALAC）共同制定。章程必须允许委员会处理涉及 SSAD 的各类运营问题。其中可能包括但不限于以下主题：服务水平协议 (SLA)、集中化/分散化、自动化、第三方目的、财务可持续性和运营/系统加强机制。GNSO 常任委员会议程应降低接受问题的门槛，确保任何参与团体都能够捍卫自身在 SSAD 运营中享有的权益并明确指出供委员会认真思考。识别问题，委员会应采取以下两种方法确定可能需要解决的问题：

i. GNSO 常任委员会成员可以提出任何与 SSAD 运营相关的政策或实施主题，如果至少有一位其他“工作组”委员会成员附议，则应列入委员会工作议程。
ii. 此外，GNSO 理事会还可以识别 SSAD 运营问题。GNSO 理事会可以选择委托 GNSO 常任委员会评估识别的问题，以便委员会向理事会提出共识性建议，即受影响的利益相关方就如何最有效地解决问题达成的共识。

关于实施指南的建议应发送给 GNSO 理事会供其审议和采纳，然后再发送给 ICANN 组织进一步推进实施工作。如果建议要求对现有 ICANN 共识性政策进行修改，应予以记录并保留，供未来制定和/或审核政策时在问题范围确定阶段使用。

18.2.3. 必要共识：GNSO 常任委员会建议的共识程度：委员会成员必须就常任委员会提出的 SSAD 运营和政策建议达成共识，而后才能将这些建议作为正式建议发送给 GNSO 理事会。为使建议达成共识，必需获得签约方的支持。为评估共识程度，广大成员需代表 SG/C 或 SO/AC 提出正式立场，而不是发表个人看法或立场。为确定共识程度，参

与达成共识性意见的各个团体（共 9 个）必须享有同等话语权，要求 CP 必须支持特定建议方可通过。

18.2.4. 解散 GNSO 常任委员会：如果需要，常任委员会可以向 GNSO 理事会提议解散常任委员会。如果常任委员会向 GNSO 理事会提议解散常任委员会，需要参与团体过半数票决通过。而后，这项建议还必需获得 GNSO 理事会采纳。

3.6 EPDP 团队第 2 优先级建议

建议 #19. 信息显示：附属和/或认证隐私/代理提供商

19.1. 如果域名注册时使用了附属和/或认证的隐私/代理服务，例如，与自然人相关的数据被屏蔽，那么注册服务机构（如果适用，还包括注册管理机构）在响应 RDDS 查询时，必须包含适用隐私/代理服务的完整 RDDS 数据。完整的隐私/代理 RDDS 数据还可能包含假名电子邮件。

实施注意事项：

19.2. 一旦 ICANN 组织实施隐私/代理服务认证计划，当建议 19 生效后，将接替或以其他方式取代 EPDP 第 1 阶段建议 14。

19.3. 本建议的目的在于向注册服务机构（和注册管理机构，如适用）提供明确的指示：即，如果通过附属和/或认证隐私/代理提供商注册域名，也不得编辑数据。工作组不支持编辑域名注册数据，也不支持提供隐私/代理服务。

建议 #20. 城市字段

EPDP 团队建议，对 EPDP 第 1 阶段建议 11 进行更新，声明可以参考注册人联系信息对城市字段进行编辑，但并非必须进行此项编辑。

建议 #21. 数据留存

EPDP 团队确认保留其在第 1 阶段提出的建议，即：注册服务机构在注册有效期后的 15 个月内，必须仅保留那些转移争议解决政策 (TDRP) 所必需的数据元素，并在此基础上增加 3 个月的数据删除时间，总计留存期为 18 个月。保留这项建议的依据是：TDRP 中有这样一项政策规定，即：根据该政策提出的投诉，只能在涉嫌违反转移政策（档案号：请参阅 TDRP 第 1.15 节）后的 12 个月内提出（档案号：请参阅 TDRP 第 2.2 节）。明确声明，此项建议不会阻止请求者（包括 ICANN 合规部在内）出于 TDRP 以外的目的请求披露这些保留的数据元素，但是，披露这些数据元素将会受到相关数据保护法律的约束，例如，披露数据是否存在法律依据。为

避免存疑，此留存期不会限制注册管理机构和注册服务机构将数据元素保留更长时间的权力。

实施指南：
为避免存疑，要求注册服务机构在注册有效期后的 15 个月保留数据，但可以在 15 个月后删除数据。

明确声明，这并不妨碍控制人出于 TDRP 以外的目的，针对控制人识别和确定的其他目的进一步延长留存期；不排除根据相关数据保护法将上述保留数据披露给任何一方。

建议 #22. 目的 2

EPDP 团队建议在 EPDP 团队第 1 阶段的目的中增加以下内容，这些内容构成新 ICANN 政策的基础：

- 根据 ICANN 使命，促进维护域名系统的安全、稳定与弹性。

3.7 EPDP 团队第 2 优先级建议结论

结论——OCTO 的职责
在考虑了这项意见后，EPDP 团队的大多数成员一致认为，在现阶段，没有必要提出额外的职责来促进 ICANN 首席技术官办公室 (OCTO) 履行其使命。之所以达成这项共识，是因为最新 ICANN 目的 2 充分介绍了 OCTO 及其他 ICANN 组织团队（如合同合规团队等）的工作使命。此外，大多数成员还一致认为，EPDP 团队决定不提出额外职责，不应阻止 ICANN 组织和/或社群确定其他职责，以便为将来可能需要访问非公开注册数据的此类未确定活动提供支持。

结论——WHOIS 准确度报告系统的准确度
根据 GNSO 理事会的指示，EPDP 团队将不会进一步审议这一主题，而是有望成立一个范围界定小组，进一步探讨与准确性和 ARS 相关的问题，以协助确定相应的后续措施来解决已确定的潜在问题。

4 后续步骤

4.1 后续步骤

本最终报告将提交至 GNSO 理事会接受审议和审批。一旦 GNSO 理事会采纳最终报告，最终报告将被提交至 ICANN 董事会进行审议，而且可能获批作为 ICANN 共识性政策。

术语表

1. 咨询委员会

咨询委员会是正规的咨询组织，由来自互联网社群的代表组成，就特定问题或政策领域为 ICANN 提供建议。有的咨询委员会是依据 ICANN 章程而设立，而有的则可能是根据需要而建立。咨询委员会在法律上无权代表 ICANN，但却向 ICANN 董事会报告调查结果并提出建议。

2. ALAC——一般会员咨询委员会

ICANN 的一般会员咨询委员会 (ALAC) 负责针对与互联网个人用户（“一般会员”社群）利益相关的各种 ICANN 活动进行考虑并提供建议。ICANN 作为一家负责在技术层面上管理互联网域名和地址系统的私营非营利性公司，将依靠 ALAC 及其支持性基础结构来涵盖并代表 ICANN 中广大互联网个人用户的利益。

3. 企业选区

企业选区代表互联网商业用户。企业选区是 ICANN 章程第 11.5 条引用的商业利益相关方团体 (CSG) 的一个选区。BC 是通用名称支持组织 (GNSO) 的一个利益相关方团体和选区，负责针对有关域名系统管理的政策问题向 ICANN 董事会提供建议。

4. ccNSO——国家和地区名称支持组织

ccNSO 是一个支持组织，负责制定与国家和地区顶级域相关的全球政策并向 ICANN 董事会提供相关建议。ccNSO 为国家和地区顶级域管理者提供了一个论坛，在此论坛中他们可以从全球视角探讨共同关切的问题。ccNSO 选出一位工作人员在董事会任职。

5. ccTLD——国家和地区顶级域

ccTLD 是由两个字母组成的域名（例如 .UK（英国）、.DE（德国）和 .JP（日本））称为国家和地区顶级域 (ccTLD)，对应于国家、地区或其他地理位置。关于采用 ccTLD 注册域名的规则和政策各不相同，并且 ccTLD 注册管理机构规定 ccTLD 仅限相应国家和地区的公民使用。

有关 ccTLD 的详细信息（包括指定 ccTLD 和主管的完整数据库），请参阅 http://www.iana.org/cctld/cctld.htm。

6. 域名注册数据

域名注册数据（也称为注册数据）是指注册服务机构或注册管理机构搜集的域名注册之时注册人提供的信息。这类信息中某些部分已经面向公众发布。现行 RAA 明确列出数据元素，以促进 ICANN 认证通用顶级域 (gTLD) 注册服务机构和注册人之间的互动。在国家和地区顶级域 (ccTLD) 方面，这类 TLD 的运营商则需根据注册信息的要求和公布条件来自行制定政策或推行政府政策。

7. 域名
域名是域名系统的一部分，用于标识互联网协议资源，如互联网网站。

8. DNS——域名系统
DNS 指互联网域名系统。域名系统 (DNS) 可帮助用户避免在互联网上“迷路”。在互联网上，每一台计算机都有唯一的地址，该地址就像电话号码一样，但却是相当复杂的一串数字。这串数字称为“IP 地址”（IP 代表“Internet Protocol”，即互联网协议）。IP 地址很难记忆。而 DNS 支持用一串熟悉的字母（即域名）来取代晦涩难记的 IP 地址，从而提高了使用互联网的便利程度。这样，不必键入 207.151.159.3，只需键入 www.internic.net 即可。域名系统 (DNS) 是一种“助记”手段，可以使地址更易于记忆。

9. EPDP——快速政策制定流程
ICANN 章程规定的一套正式程序，为那些用以协调全球互联网唯一标识符系统的政策的发起、内外部审查、推行时机和批准提供指导。GNSO 理事会仅可在以下具体条件下启动 EPDP：(1) 解决 ICANN 董事会采用 GNSO 政策建议或执行该被采用的建议之后确认并确定范围的狭义的政策问题；或 (2) 为某一具体政策问题提出新的或附加的政策建议，该政策问题的大致范围事先已基本确定，相关背景信息已存在，例如，(a) 出现在关于某次未启动的潜在 PDP《问题报告》中；(b) 作为之前某次未完成的 PDP 的一部分；或 (c) 贯穿于其他项目中，例如 GNSO 指导流程。

10. GAC——政府咨询委员会
GAC 是一个咨询委员会，成员包括来自各国政府、跨国政府机构和公约组织以及不同经济体的指定代表。其职能是就各国政府关心的问题向 ICANN 董事会提出建议。GAC 将发挥论坛作用，汇集围绕政府利益及关注点（包括消费者利益）的讨论。作为咨询委员会，GAC 在法律上无权代表 ICANN，但会向 ICANN 董事会报告调查结果并提供建议。

11. 通用数据保护条例 (GDPR)
通用数据保护条例 (EU) 2016/679 (GDPR) 是欧盟法律面向欧盟 (EU) 和欧洲经济区 (EEA) 全体公民出台的数据保护和隐私法规。同时还就向欧盟和 EEA 以外地区输出个人数据进行了规范。

12. GNSO——通用名称支持组织
支持组织，负责制定与通用顶级域相关的实质性政策并上报 ICANN 董事会。其成员包括 gTLD 注册机构、gTLD 注册商、知识产权利益主体、互联网服务提供商 (ISP)、企业和非商业利益主体委派的代表。

13. 通用顶级域 (gTLD)
“gTLD”是指 ICANN 根据具有充分效力的注册管理机构协议授予的 DNS 顶级域，但国家和地区 TLD (ccTLD) 或国际化域名 (IDN) 国家和地区 TLD 除外。

14. gTLD 注册管理机构利益相关方团体 (RySG)
gTLD 注册管理机构利益相关方团体 (RySG) 是根据互联网名称与数字地址分配机构 (ICANN) 章程第 X 条第 5 节（2009 年 9 月）成立的通用名称支持组织 (GNSO) 中的一家公认实体。

RySG 的主要职责是代表以下 gTLD 注册管理运行机构（对于赞助性 gTLD，是指赞助商）（“注册管理机构”）的利益：(i) 目前与 ICANN 签署合同，提供 gTLD 注册管理机构服务，为一个或多个 gTLD 提供支持；(ii) 同意受合同中提出的共识性政策的约束；(iii) 自愿选择成为 RySG 成员。RySG 可以包括第 IV 条定义的利益团体。RySG 代表 RySG 向 GNSO 理事会和 ICANN 董事会提出的观点，尤其侧重于与互联网或者域名系统的互操作性、技术稳定性和稳定运营相关的 ICANN 共识性政策。

15. ICANN——互联网名称与数字地址分配机构
互联网名称与数字地址分配机构 (ICANN) 是一家非营利性国际机构，负责分配互联网协议 (IP) 地址空间，指定协议标识符，管理通用顶级域 (gTLD) 系统、国家和地区顶级域 (ccTLD) 系统及根服务器系统。最初，互联网号码分配机构 (IANA) 和其他实体按照美国政府合同执行这些服务。ICANN 目前行使 IANA 的职能。作为一家公私合作机构，ICANN 致力于维护互联网的运营稳定性、鼓励竞争、实现全球互联网社群的广泛参与、并通过自下而上的共识性流程制定合理政策，履行该组织的使命。

16. 知识产权选区 (IPC)
知识产权选区 (IPC) 代表 ICANN 全球知识产权社群的观点和权益，重点关注商标、版权和相关知识产权以及它们与域名系统 (DNS) 的相互影响和相互作用。IPC 是通用名称支持组织 (GNSO) 的一个选区团体，负责针对有关域名系统管理的政策问题向 ICANN 董事会提供建议。

17. 互联网服务提供商和连接提供商选区 (ISPCP)
ISP 和连接提供商选区是 GNSO 的一个选区。该选区的目标是在 ICANN 持续推进组织活动时履行相关 ICANN 和 GNSO 章程、规则或政策规定的角色和职责。ISPCP 旨在确保互联网服务提供商和连接提供商选区的观点有助于实现 ICANN 的目的和目标。

18. 域名服务器
域名服务器是一个 DNS 组件，用于存储 DNS 域名空间中一个（或多个）区域的信息。

19. 非商业利益相关方团体 (NCSG)
非商业利益相关方团体 (NCSG) 是 GNSO 中的一个利益相关方团体。非商业利益相关方团体 (NCSG) 的目的是通过当选代表及其选区代表通用顶级域 (gTLD) 非商业注册人和非商业互联网用户的利益和诉求。旨在为以下团体和个人提供 ICANN 流程发言权和代表权：代表非商业利益的非营利性组织；非营利性服务，如教育、慈

善事业、消费者保护、社群组织、艺术推广、公共利益政策宣传、儿童福利、宗教、科学研究和人权；公益软件问题；注册用于非商业个人用途的域名的家庭或个人；以及主要关注域名政策非商业公共利益层面的互联网用户。

20. 授权后争议解决程序 (PDDRP)
授权后争议解决程序旨在为那些被新 gTLD 注册管理运行机构的行为伤害的人士提供投诉途径。所有此类争议解决程序均由 ICANN 外部提供商负责运转，要求投诉人在提交正式投诉之前采取具体措施解决面临的问题。由专家小组确定注册管理运行机构是否有错，并向 ICANN 提供纠正建议。

21. 注册域名
“注册域名”指 gTLD 域中的域名，由两 (2) 级或多级（例如 john.smith.name）组成，对于该注册域名，gTLD 注册管理执行机构（或参与提供注册管理机构服务的附属机构或分包商）在注册管理机构数据库中维护其相关数据、安排此类维护或通过此类维护获取收入。注册管理机构数据库中的域名即使没有出现在区域文件中，也可能是注册域名（例如已注册但未使用的域名）。

22. 注册服务机构
“注册服务机构”一词若不加引号，则指与注册域名持有人以及注册管理执行机构签订合同，收集有关注册域名持有人的注册资料，并提交注册信息以输入注册管理机构数据库的个人或实体。

23. 注册服务机构利益相关方团体 (RrSG)
注册服务机构利益相关方团体是 ICANN 社群中的若干利益相关方团体之一，而且是注册服务机构的代表机构。它是一个多元化活跃团队，致力于有效维护注册服务机构及其客户的利益。我们诚邀大家深入了解认证域名注册服务机构及其在域名系统中扮演的重要角色。

24. 注册管理运行机构
“注册管理执行机构”指负责为特定 gTLD 提供注册管理机构服务的个人或实体，其服务依据为 ICANN（或其代理人）与该个人或实体之间的协议，如果该协议终止或失效，则依据美国政府与该个人或实体之间的协议提供服务。

25. 注册数据目录服务 (RDDS)
域名注册数据目录服务 (RDDS) 是指注册管理机构和注册服务机构针对域名注册数据提供访问功能的一种服务。

26. 注册限制争议解决程序 (RRDRP)
注册限制争议解决流程 (RRDRP) 专门用于解决基于社群的新通用顶级域注册管理运行机构没有遵守其《注册管理机构协议》中规定的注册限制的情况。

27. SO——支持组织

SO 是就域名（GNSO 和 CCNSO）和 IP 地址 (ASO) 相关问题向 ICANN 董事会提供建议的三个专门性咨询机构。

28. SSAC——安全与稳定咨询委员会

一个服务于 ICANN 董事会的咨询委员会，由来自业界、学术界、互联网根服务器运营商、注册服务机构和 TLD 注册管理机构的技术专家组成。

29. TLD——顶级域

TLD 是 DNS 命名级别中最高层次的域名。它们在域名中显示为最后（最右面）的“.”之后的字母串，例如 http://www.example.net 中的“net”。TLD 的管理者负责控制该 TLD 下识别哪些二级域名。根域或根区域的管理者负责掌管哪些 TLD 能被 DNS 识别。常用的 TLD 有 .COM、.NET、.EDU、.JP、.DE 等。

30. 统一争议解决政策（UDRP）

统一域名争议解决政策 (UDRP) 是一种权利保护机制，规定注册服务机构用于解决 gTLD 域名注册及使用相关争议的程序和规则。UDRP 提供了强制性管理程序，主要用于处理滥用性恶意域名注册索赔。UDRP 仅适用于处理注册人与第三方之间的争议，而不适用于处理注册服务机构与其客户之间的争议。

31. 统一快速中止程序 (URS)

统一快速中止系统是一种权利保护机制，为面临着明确侵权问题的权利持有人提供更快速、更经济的缓和措施，从而对现行统一域名争议解决政策 (UDRP) 进行补充。

32. WHOIS

WHOIS 协议是一个互联网协议，用于查询数据库以获取某域名的注册信息（或 IP 地址）。WHOIS 协议最初是在 1985 年发布的 RFC 954 中作出规定，其最新规定记载于 RFC 3912 中。ICANN 的 gTLD 协议要求注册管理机构和注册服务机构提供一个互动网页和一个 WHOIS 服务端口 43，让公众免费访问已注册域名的相关数据。此类数据通常称为“WHOIS 数据”，包含诸如域名注册时间和到期时间、名称服务器、注册人联系信息、指定管理及技术联络人的联系信息等要素。

WHOIS 服务通常用于识别商用域名的持有人，以及识别能够更正已注册域名的技术问题的相关方。

附录 A——非公开注册数据标准化访问/披露系统——背景信息

问题描述和/或章程问题

摘自 EPDP 团队章程：

(a) 访问数据的目的——尚未解答但将提供实施指导的政策问题是什么？

a1) 根据适用法律，第三方访问注册数据的合法目的是什么？

a2) 支持这一访问的法律依据是什么？

a3) 访问非公开注册数据的资格标准是什么？

a4) 这些相关方/团体是否包括不同性质的第三方请求者？

a5) 用户/相关方可基于自身目的访问哪些数据元素？

a6) 我们可以在多大程度上确定一组数据元素及针对特定第三方和/或目的的潜在范围（数量）？

a7) 具备技术能力的 RDAP 如何使注册管理机构/注册服务机构接受认证标记和查询目的？当相应认证机构开发认证模型并获得相关法律机构的批准后，如何才能确保 RDAP 具备技术能力，而且随时可以接受、记录和响应认证请求者的标记？

(b) 资格审查——尚未解答但将提供实施指导的政策问题是什么？

b1) 如何授予和管理凭据？

b2) 谁负责提供凭证？

b3) 如何将这些凭证集成到注册服务机构/注册管理机构的技术系统中？

(c) 访问条款和使用条款合规性——尚未解答但将提供实施指导的政策问题是什么？

c1) 监管用户数据访问的规则/政策是什么？

c2) 一旦访问，监管用户数据使用的规则/政策又是什么？

c3) 谁负责制定和执行这些规则/政策？

c4) 如果用户滥用数据，将面临哪些制裁或处罚？除适用法律规定的制裁以外，还包括未来对数据遭到滥用的数据主体实施访问或赔偿限制。

c5) 签约方将对访问的数据类型和数据的使用方式具有哪些认识？

c6) 数据主体在确定何时及如何访问和使用个人数据方面具有哪些权利？

c7) 第三方访问模型如何适应数据主体的不同数据披露通知要求？

摘自临时规范附录：

- 设法向潜在 URS 和 UDRP 投诉人提供充分的注册数据访问权限，支持本着诚信的态度提交投诉。
- 认证计划设想的查询量与现实调查交叉引用需求保持均衡面临的限制。
- 对执法机构查询注册数据保密。
- 根据第 4.4 节规定，继续推进社群工作，开发符合 GDPR 的认证和访问模型，同时认识到亟需向第 29 条工作组/欧洲数据保护理事会寻求进一步指导。
- 在最终认证和访问机制全面正常运行之前，强制要求所有签约方采取统一流程，确保用户能够出于合法目的继续访问注册数据，包括非公开数据。

摘自 EPDP 团队第 1 阶段最终报告：

EPDP 团队建议 3。
根据 EPDP 团队章程和目的 2，既然章程中的基础问题已得到回答，EPDP 团队承诺就用于合法披露非公开注册数据的标准化模型（章程中称之为“标准化访问”）提出建议。这涉及解决几方面的问题，例如：

- 是否应采用此类系统？
- 第三方访问注册数据的合法目的是什么？
- 访问非公开注册数据的资格标准是什么？
- 这些相关方/团体是否包括不同性质的第三方请求者？
- 用户/相关方可访问哪些数据元素？

除其他问题外，在这种背景下，EPDP 团队还将考虑知识产权侵权和 DNS 滥用过程中的披露。必需确认出于合法目的的披露与收集此类数据的目的并不矛盾。

TSG 政策问题

1. EPDP 或其他政策倡议在非公开 gTLD 域名注册数据访问方面取得的成效。
2. 识别并选择可以授予系统使用凭证的身份供应商（如果已做出选择）。[45]
3. 描述获得非公开 gTLD 域名注册数据访问权限的请求者的基本资格，例如，哪些类型的请求者可以访问哪些非公开 gTLD 域名注册数据字段（“授权策略”）。
4. 详细说明只有特定类别的请求者可以下载活动日志，还是一般请求者均可下载活动日志。
5. 描述对各系统组件施加的数据留存要求。

[45]有些代表指出，此类问题可能不属于 EPDP 团队的职责范围。

6. 描述各系统组件的服务水平要求 (SLR)，包括这些 SLR 和组件运营商评估是否公开并用于处理访问投诉。
7. 指定拒绝请求的合理原因。
8. 简要介绍匿名查询关联支持，如第 7.2 节所述。
9. 简要介绍第 8 节中所述的参与者模型选择方法，以及第 10.1 至 10.5 节中所述的相应支持组件和服务发现。
10. 描述向 CP 披露请求的条件（如果有）。
11. 提供关于各系统组件的运营商责任的法律分析。
12. 简要介绍提交不当披露投诉的程序及相应的可接受使用策略。

预期交付成果

关于合法披露/访问非公开注册数据的标准化模型的政策建议

常规必读文献

描述	链接	必读原因
持续访问完整 WHOIS 数据的统一访问模型框架元素（2018 年 6 月 18 日）	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf	
非公开 WHOIS 数据认证和访问模型草案 (BC/IPC)	2018 年 7 月 23 日，模型版本 1.7	
Palage 差异化注册人数据访问模型（又名 Philly Special）	Palage 差异化注册人数据访问模型（又名 Philly Special）- 2018 年 5 月 30 日，版本 2.0	

持续访问完整 WHOIS 数据的统一访问模型——社群提交模型比较（2018 年 6 月 18 日）	https://www.icann.org/en/system/files/files/draft-unified-access-model-summary-elements-18jun18-en.pdf	
关于将数据保护原则应用于 WHOIS 目录的第 29 条 WP 意见 2/2003（2003 年）	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf	
EWG 报告第 4c 节，RDS 用户认证原则（2014 年 6 月）	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf	
EWG 研究– RDS 用户认证 RFI	https://community.icann.org/download/attachments/45744698/EWG%20USER%20ACCREDITATION%20RFI%20SUMMARY%2013%20March%202014.pdf	
第一部分：工作原理：RDAP – 2019 年 3 月 10 日	https://64.schedule.icann.org/meetings/963337	
第二部分：了解 RDAP 及其在 RDDS 政策中可以扮演的角色 – 2019 年 3 月 13 日	https://64.schedule.icann.org/meetings/961941	
非公开注册数据访问技术研究组拟定的非公开注册数据访问技术模型（2019 年 4 月 30 日）	TSG01，非公开注册数据访问技术模型	
隐私和代理服务认证问题最终报告（2015 年 12 月 7 日） • 定义 – 第 6-8 页	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	

• 附录 B——适用于知识产权持有人披露请求的说明性披露框架 – 第 85 – 93 页 • 隐私和代理服务提供商认证协议草案		

即将发布的简报

主题	可能的演示者	重要原因
RDAP——ICANN65 会议问答环节后期审核	弗朗西斯科 • 阿瑞亚斯 (Francisco Arias)，ICANN 组织	确保对 RDAP 的工作和职能形成共同的认识

依赖条件

描述依赖条件	依赖于	预计或建议时间
根据第 1 阶段报告协商并最终确定必要的数据保护协议是开展大部分第 2 阶段工作的先决条件（ISPCP 建议）	CP/ICANN 组织	

拟定时间安排和方法

简介

EPDP 团队的目标是制定与请求方共享非公开注册数据的政策建议并达成一致意见[46]（非公开注册数据标准化访问/披露系统）。

[46] 摘自 EPDP 第 1 阶段最终报告：“注册数据”是指 [EPDP 第一阶段最终报告] 附录 D 中确定的数据元素，此类数据元素从与域名注册相关的自然人和法人收集而来。

在出台令相关方满意的法律保证之前，提出标准化披露/访问系统政策建议将与系统形态无关。

同时，EPDP 团队应从整体上与 ICANN 组织合作提出政策问题，这将有助于与 DPA 开展讨论，DPA 的目标是确定哪种标准化披露系统模型完全符合 GDPR、可行并有利于解决/减轻签约方的法律责任。

预计将阐述以下主题（列表并不完整）：

- 术语和工作定义
- 必要法律指导意见
- 要求，包括定义用户组、请求标准和标准/内容
- 发布必要流程、标准和内容要求
- 流程时间表
- 回执
- 认证
- 身份验证和授权
- 第三方披露目的
- 披露的法律依据
- 可接受的使用策略
- 使用条款/披露协议，包括履行法律要求
- 隐私政策
- 查询策略
- 数据的保留与销毁
- 服务水平协议
- 财务可持续性

方法

首先确定：

a) 术语和工作定义
b) 寻求必要法律指导意见（注意，这也是贯穿所有主题的一项持续活动）。

讨论其余主题的可能逻辑顺序：

c) 定义用户组、每个用户组的标准和目的/法律依据
↓
d) 针对用户组进行核实/授权/认证
↓

e) 每个用户组的请求标准/内容
↓
f) 查询策略
↓
g) 回执，包括时间表
↓
h) 响应要求/预期，包括时间表/SLA
↓
i) 可接受的使用策略
↓
j) 使用条款/披露协议/隐私政策
↓
k) 数据的保留与销毁

l) 总体审议主题：财务可持续性

下文进一步详细介绍了各项主题。要跳转到各个部分，请使用以下链接：

完成本工作表及其他工作表后，每个主题（包括第 1 阶段主题）及其工作范围将为实施总体调度工作计划奠定基础。一些主题可以并行处理，另一些主题可能需要依赖其他工作才能进行更深入的考量。每个主题都会预留一定的时间进行问题审议、得出可能的结论和/或就政策问题提出可能的建议。一旦获得整体支持，结论或建议将用于进一步审议和完善初步报告。目标是在发布前尽量就提案达成共识。

a) 主题：术语和工作定义

目标：为确保与本讨论中使用的术语意义一致并避免混淆，EPDP 团队就一系列工作定义达成共识。据了解，这些工作定义仅用于澄清使用的术语，不是为了限制工作范围或预先确定结果。人们理解，流程结束后，需要对这些工作定义进行审核和修订。

需要审核的材料：

- GDPR 和其他数据保护法规中使用的术语
- 隐私和代理服务认证问题最终报告（2015 年 12 月 7 日）- 电子定义 - 第 6-8 页

相关思维导图问题：无

相关 EPDP 第 1 阶段实施问题：有待确定 - 建议 18 实施可能包括一些定义，或许需要列入 EPDP 小组第 2 阶段审议议程。

任务：

- 确认实施建议 18 时预计是否要创建或应用任何定义（员工）
- 编制工作定义第一稿（员工）
- 通过 EPDP 团队审核并提出意见 (EPDP)
- 就一组基本定义达成一致意见 (EPDP)
- 通过审议创建定义工作文件（全部）

目标完成日期：2019 年 5 月 30 日

b) 主题：法律问题

目标：识别有助于在 EPDP 团队审议本主题时作为依据的法律问题。

截至目前提交的问题：

问题	状态	所有者
1.必需确认出于合法目的的披露与收集此类数据的目的并不矛盾。	已暂停 第 2 阶段 LC 指出，此时考虑这个问题还为时尚早，因而将问题标记为“已暂停”。当 EPDP 团队确定披露目的后再重新讨论这个问题。	
2.解答非公开注册数据标准化访问系统面临的控制权和法律问题，假设采用的技术框架与 TSG 一致，而且可以充分解决责任和风险缓解相关问题，目标在于采用标准化访问 (IPC) 系统降低签约方的责任风险。	修订 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	
3.寻求法律指导意见，确定建立基于认证的披露系统的可行性。(ISPCP)	已暂停 第 2 阶段 LC 指出，此时考虑这个问题还为时尚早，因而将问题标记为“已暂停”。当 EPDP 团队确定披露目的后再重新讨论这个问题。	
4.应将根据 GDPR 第 6 I f 条披露给非欧盟执法机构的问题提交法律顾问。(ISPCP)	修订	

	第 2 阶段 LC 正在向提出此问题的人员寻求进一步的指导，完成指导意见和/或更新内容审核后，确定是否应将问题提交至外部顾问。	
5. 可不可以设计集中式访问/披露模型（在模型中，一家实体负责接收披露要求、执行平衡测试、核实认证状态、做出请求响应等），以期最大限度地限制签约方责任？也就是，可不可以这样认为：中央实体可以在很大程度上（哪怕不是全部）负责履行披露相关责任（包括认证和授权），而且可以将签约方责任严格限定于除披露以外的其他处理活动，如数据收集和安全传输？如果可以，需要从政策层面进行哪些考量/阐述以便适应这一需求？(ISPCP)	修订 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	
6. 在 SSAD 中，除自行确定披露数据的法律依据以外，被请求者（掌握请求数据的实体）是否需要对第三方请求者的法律依据进行评估？（ICANN65 会议期间 GAC/IPC 提出的问题）	修订 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	
7. 当第三方曲解预期处理方法时，签约方应负多大责任（如果有的话）？如何减轻这种责任？(BC)	修订 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	

8. BC 建议 EPDP 将目的 2 划分为两项独立目的： • 通过控制和处理 gTLD 注册数据，使 ICANN 能够根据 ICANN 使命和章程维护域名系统的安全、稳定与弹性。 • 支持第三方解决涉及域名使用或注册的消费者保护、网络安全、知识产权、网络犯罪和 DNS 滥用问题。咨询顾问，确定重申的目的 2 是否正确（如上所述） 可不可以咨询法律顾问确定：重申的目的 2（如上所述）是否符合 GDPR？如果无法使用上述语言，顾问是否可以提出语言改进建议？(BC)	**已暂停** 第 2 阶段 LC 指出，此时考虑这个问题还为时尚早，因而将问题标记为“已暂停”。当 GNSO 理事会和董事会协商回复“建议 1 目的 2 已完成”后，将重新讨论这个问题。	
9.可不可以就以下两方面进行法律分析：如何执行 6(1)(f) 提出的平衡测试？在哪种情况下，6(1)(f) 可能需要手动审查请求？(BC)	**修订** 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	
10.倘若并非所有请求都适合手动审核，是否可以通过某种法律方法定义请求类别（例如，快速响应恶意软件攻击或联系没有回应的 IP 侵权者）来降低手动审核需求？(BC)	**修订** 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	
11.可不可以咨询法律顾问确定：GDPR 是否会阻止已议定适当保护措施且获得相应资质的网络安全专业人员大规模访问？倘若不禁止此类访问，顾问可不可以举例说明应考虑实施的保护措施（如匿名化机制）？(BC)	**修订** 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	

12.为将第 6(1)(b) 节列为注册数据处理目的，应遵循 B&B 建议：“至少从理论上而言，务必要求签署合同时数据主体了解特定第三方，或者至少了解第三方执行的处理操作。同时，要求作为签约合作伙伴的控制人，在向第三方传输数据之前通知数据主体” B&B 应该澄清为何认为提供 WHOIS 的唯一依据是防止 DNS 滥用。第 10 款得出的结论未考量 EPDP 在建议 1 中确定的其他目的；而且，无论在任何情况下，均应考量 EC 近期提出的 ICANN 的广泛目的： “根据 ICANN 使命，促进维护域名系统的安全、稳定与弹性”，这是 ICANN 作为域名系统“守护人”的核心职责。	修订 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	
13. 鉴于 EC 认识到以下问题，B&B 应在 GDPR 公共利益 6(1)e 部分适用的范围内提出建议： “在确定目的 2 时，欧盟委员会承认 ICANN 在保障互联网域名系统安全、稳定与弹性方面承担的核心角色和职责，而且这种做法符合公共利益。”	修订 第 2 阶段 LC 正在对问题措辞进行修改，完成更新内容审核后，确定是否应将问题提交至外部顾问。	

任务：

- 确定第 2 阶段相关主题的优先级问题
- 议定处理审议过程中出现的各类问题的方法和批准流程

目标完成日期：进行中

c) 主题：定义用户组、每个用户组的标准和目的/法律依据

目标：

- 定义可能请求披露/访问非公开注册数据的用户组类别，以及确定个人或实体是否属于该类别所依据的标准。
- 确定每个用户组处理数据的目的和法律依据

- 确定第 2 阶段标准化框架是否以及如何满足大型工作组所特有的请求。如果用户不符合所有既定用户组的要求，考量其是否仍可通过实施建议 18 或其他方式请求披露/访问。

相关思维导图问题：

P1-Charter-a
(a) 访问数据的目的——尚未解答但将提供实施指导的政策问题是什么？
a1) 根据适用法律，第三方访问注册数据的合法目的是什么？
a2) 支持这一访问的法律依据是什么？
a3) 访问非公开注册数据的资格标准是什么？
a4) 这些相关方/团体是否包括不同性质的第三方请求者？

临时规范附录：
3. 设法向潜在 URS 和 UDRP 投诉人提供充分的注册数据访问权限，支持本着诚信的态度提交投诉。

第 1 阶段建议
EPDP 团队建议 3
- 第三方访问注册数据的合法目的是什么？
- 访问非公开注册数据的资格标准是什么？
- 这些相关方/团体是否包括不同性质的第三方请求者？

EPDP 团队要求，当 EPDP 团队在标准化访问框架内开始着手考量时，一名 RPM PDP 工作组的代表应提供关于当前考量状态的最新信息，以便 EPDP 团队确定在标准化访问框架考量的背景下，工作组的建议是否会影响对 URS 和 UDRP 的考虑，以及如何影响。

注意，目的 2 预留了空间，等待就 EPDP 第 2 阶段的访问问题开展进一步工作，预计将在完成第 2 阶段工作后重新讨论。[工作人员注意事项——与目的有关，但在完成第 2 阶段工作后才会安排重新讨论目的 2]

TSG-Final-Q#3
3. 描述获得非公开 gTLD 域名注册数据访问权限的请求者的基本资格，例如，哪些类型的请求者可以访问哪些非公开 gTLD 域名注册数据字段（“授权策略”）。

需要审核的材料：

描述	链接	必读原因
2017 年 6 月末，ICANN 要求签约方和感兴趣的利益相关方确定 ICANN 政策和合同所要求的用户类型和数据元素用途。下文提供了收到的个人响应和响应汇编。	数据流矩阵，收到的响应汇编——当前版本	近期开展的用户类型识别工作
EWG 最终报告对现有的 WHOIS 系统用户进行了简单总结，包括本着建设性目的或恶意目的的用户。根据 EWG 任务，对所有这些用户进行了审查，确定现有流程、可能的未来工作流程以及涉及的利益相关方和数据。	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf -第 20-25 页	
审核 EPDP 团队第 1 阶段提出的目的及确定的法律依据	Https://gnso.icann.org/en/drafts/epdp-gtld-registration-data-specs-final-20feb19-en.pdf（34-36（第 34-36 页/第 67-71 页）	
GDPR 相关规定	GDPR 相关规定——请参阅第 6(1)、6(2) 和 40 条	
ICO 处理信息页面的法律依据	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/	

相关 EPDP 第 1 阶段实施问题：
暂无

任务：

- 根据源材料制作第一个请求者类别列表。（员工）
- 审核请求者类别列表并确定资格标准。（全部）
- 开发滥用类型和场景以形成用例，确定每一位请求者的要求
- 确定每个用户组处理数据的目的和法律依据（全部）
- 确定第 2 阶段标准化框架是否以及如何满足大型工作组所特有的请求。如果用户不符合所有既定用户组的要求，考量其是否仍可通过实施建议 18 或其他方式请求披露/访问。（全部）
- 确认章程中提出的所有问题均已得到解决和记录。

目标完成日期：2019 年 6 月 13 日
（重新讨论目的 2——第 2 阶段工作完成后）

d) 针对用户组进行核实/授权/认证

目标：

- 确定是否需要对用户组进行核实、授权和/或认证
  - 认证模型可以与 EPDP 第 1 阶段建议 18 中实施的认证模型互补或搭配使用吗？
- 如果可以，请制定核实、授权和/或认证政策原则，包括解决以下问题：
  - 如果用户在通过验证后请求访问非公开 WHOIS 数据，是否必须针对每一项查询/请求提供合法权益。
- 如果不需要，解释相关原因以及可能会对特定用户组的查询（如果有）产生的影响。

相关思维导图问题：

P1-Charter-a/b

(a) 访问数据的目的——尚未解答但将提供实施指导的政策问题是什么？
a7) 具备技术能力的 RDAP 如何使注册管理机构/注册服务机构接受认证标记和查询目的？当相应认证机构开发认证模型并获得相关法律机构的批准后，如何才能确保 RDAP 具备技术能力，而且随时可以接受、记录和响应认证请求者的标记？

(b) 资格审查——尚未解答但将提供实施指导的政策问题是什么？
b1) 如何授予和管理凭据？
b2) 谁负责提供凭证？
b3) 如何将这些凭证集成到注册服务机构/注册管理机构的技术系统中？

临时规范附录

1. 根据第 4.4 节规定，继续推进社群工作，开发符合 GDPR 的认证和访问模型，同时认识到亟需向第 29 条工作组/欧洲数据保护理事会寻求进一步指导。

TSG-Final-Q#2

识别并选择可以授予系统使用凭证的身份供应商（如果已做出选择）。

需要审核的材料：

描述	链接	必读原因
在 TSG 模型中识别并核实身份	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf 第 23-24 页	
EWG 最终报告——RDS 联系信息使用授权和 RDS 用户认证原则	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf 第 39-40 页和第 62-67 页	
持续访问完整 WHOIS 数据的可能统一访问模型框架 草案——如何制定合法用户身份验证要求？	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf 第 9-10、10-11、18、23 页	

相关 EPDP 第 1 阶段实施问题：

暂无。

任务：

- 查看上方列出的材料，讨论核实/授权意见。(EPDP)
- 确认关键术语“授权、认证和核实”的定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：ICANN 65

e) 每个用户组的请求标准/内容

目标：为 c 款下确定的每个用户组确定最低策略要求、标准和内容。

相关思维导图问题：

P1-Charter-c
c1) 监管用户数据访问的规则/政策是什么？

需要审核的材料：

描述	链接	必读原因
• 附录 B——适用于知识产权持有人披露请求的说明性披露框架——第 85 – 93 页 • 隐私和代理服务提供商认证协议	隐私和代理服务认证问题最终报告（2015 年 12 月 7 日）	
示例：.DE 信息和申请表	https://www.denic.de/en/service/whois-service/third-party-requests-for-holder-data/ https://www.denic.de/fileadmin/public/downloads/Domaindatenanfrage/Antrag_Domaindaten_Rechteinhaber_EN.pdf	

示例：Nominet 申请表	https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2018/05/22101442/Data-request-form.pdf	

相关 EPDP 第 1 阶段实施问题：

建议 18（但不需要自动披露信息）

合法披露的合理请求的最低信息要求：

- 识别请求者信息（包括企业实体或个人的性质/类型、授权书声明，如适用并相关）；
- 关于请求者的法律权限、特定请求依据和/或理由（例如，请求的依据或理由是什么？为何请求者需要请求此数据？）；
- 确认秉承诚信的原则提出请求；
- 请求者请求的数据元素列表以及为何仅限基于“必需”原则访问此数据；
- 同意合法处理响应请求期间收到的任何数据。

任务：

- 确认建议 18 的实施方法
- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：ICANN 65

f) 查询策略

目标：制定查询日志记录最低策略要求，定义用于控制何时可以使用查询日志的适当控件，确定是否对经过身份验证和未经身份验证的 SSAD 用户设置查询限制。

- 如何限制访问非公开注册数据，最大程度地缓解未经授权的访问和使用风险（例如，仅启用基于特定查询的访问，而不是批量传输和/或其他搜索限制或反向目录服务，包括基于实现相关合法目的的“必需”原则限制字段访问的机制）？
- 是否应考量查询机密性，例如执法机构？

- 如何平衡查询限制与实际调查交叉引用需求？

相关思维导图问题：

P1-Charter-a
a7) 具备技术能力的 RDAP 如何使注册管理机构/注册服务机构接受认证标记和查询目的？当相应认证机构开发认证模型并获得相关法律机构的批准后，如何才能确保 RDAP 具备技术能力，而且随时可以接受、记录和响应认证请求者的标记？

临时规范附录：
6 认证计划设想的查询量与现实调查交叉引用需求
保持均衡面临的限制。
7 对执法机构查询注册数据保密。

需要审核的材料：

描述	链接	必读原因
SSAC 101——关于访问域名注册数据的 SSAC 公告	https://www.icann.org/en/system/files/files/sac-101-en.pdf	描述速率限制的影响。

相关 EPDP 第 1 阶段实施问题：无。

任务：
- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：ICANN 65

g) 回执，包括时间表

目标：制定回执时间表政策要求及回执应满足的其他要求（如果有）。

注册服务机构/注册管理机构最低标准回执的基本要求（如果有）是什么？“紧急”请求呢？如何进行定义？

相关思维导图问题：

P1-Charter-c
c1) 监管用户数据访问的规则/政策是什么？

需要审核的材料：

描述	链接	必读原因
第 1 阶段最终报告建议 18 注册服务机构和注册管理运行机构响应时间表和标准	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf，第 19 页	

相关 EPDP 第 1 阶段实施问题： - 建议 18：
注册服务机构和注册管理运行机构响应时间表和标准 -
注册服务机构和注册管理机构必须合理考量合法披露并满足合法披露请求：
• 合法披露的合理请求回执的响应时间。除非有特殊情况，否则不得无故延误，但不得超过收到后的两 (2) 个工作日。

任务：
- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：待定

h) 响应要求/预期，包括时间表/SLA

目标：围绕响应要求制定政策要求，包括解决以下问题：

- 涉及解决几方面的问题，例如：
  - 经过身份验证的用户执行查询时是否必须返回完整 WHOIS 数据。
  - SLA 应对访问/披露请求响应做出什么样的承诺
  - 响应请求（包括拒绝请求）的最低要求是什么？

相关思维导图问题：

P1-Charter-a/c
a5) 用户/相关方可基于自身目的访问哪些数据元素？
a6) 我们可以在多大程度上确定一组数据元素及针对特定第三方和/或目的的潜在范围（数量）？
c1) 监管用户数据访问的规则/政策是什么？

第 1 阶段建议 3
用户/相关方可访问哪些数据元素？

临时规范附录
2.解决要求唯一联系人对给定注册服务机构的所有域名注册使用统一匿名电子邮件地址的可行性，同时确保安全性/稳定性并满足附录 A 第 2.5.1 节的要求。

TSG-Final-Q#6
描述各系统组件的服务水平要求 (SLR)，包括这些 SLR 和组件运营商评估是否公开并用于处理访问投诉。
TSG-Final-Q#7
指定拒绝请求的合理原因。
TSG-Final-Q#8
简要介绍匿名查询关联支持，如第 7.2 节所述。

需要审核的材料：

描述	链接	必读原因
第 1 阶段最终报告建议 18 注册服务机构和注册管理运行机构响应时间表和标准	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf，第 19 页	
隐私和代理服务认证问题最终报告（2015 年 12 月 7 日） • 附录 B——适用于知识产权持有人披露请求的说明性披露框架——第 90-92 页	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	PPSAI 说明性披露框架部分，详细介绍最低响应要求

相关 EPDP 第 1 阶段实施问题：
建议 18：

- 信息响应应包括的要求。如果拒绝披露（全部或部分）数据，应在响应中提供足以使请求者理解做出拒绝决定的理由，例如分析和解读平衡测试应用方法（如适用）。
- 应按照标准业务备案惯例保留请求、确认和响应日志，以便根据需要进行生成日志，包括但不限于满足 ICANN 合规部门审核需求；
- 除非遇到特殊情况，否则应及时对请求者做出响应，不得无故延误，最多不得超过 30 天。此类情况可能需要统计收到的请求总数。签约方将定期向 ICANN 报告收到的请求数量，以便评估其合理性。
- 考虑对“紧急”合理披露请求采用单独的时间表 [少于 X 个工作日]，针对这些请求提供证据，表明需要立即披露请求 [实施阶段将最终确定时间范围并制定紧急请求标准]。

任务：

- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：8 月

i) 可接受的使用策略

目标：围绕以下方面制定政策要求：

1. 应如何制定、不断完善和执行行为准则（如果有）？
2. 如果 ICANN 及其签约方为具有合法利益的第三方制定行为准则，应考虑哪些特色和需求？
3. 除第 1 阶段所记录的内容以外，是否还必须记录其他数据流？
行为准则可以与 EPDP 第 1 阶段建议 18 中实施的行为准则互补或搭配使用吗？

相关思维导图问题：

P1-Charter-c
c1) 监管用户数据访问的规则/政策是什么？
c2) 一旦访问，监管用户数据使用的规则/政策又是什么？
c3) 谁负责制定和执行这些规则/政策？

c4) 如果用户滥用数据，将面临哪些制裁或处罚？
除适用法律规定的制裁以外，还包括未来对数据遭到滥用的数据主体实施访问或赔偿限制。
c5) 签约方将对访问的数据类型和数据的使用方式具有哪些认识？
c6) 数据主体在确定何时及如何访问和使用个人数据方面具有哪些权利？
c7) 第三方访问模型如何适应数据主体的不同数据披露通知要求？

需要审核的材料：

描述	链接	必读原因
GDPR 第 40 条，行为准则	https://gdpr-info.eu/art-40-gdpr/	
第 29 条工作组致 ICANN 的信函 2018 年 4 月 11 日	https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf	
Bird & Bird——行为准则和认证参考材料（2017 年 5 月）	https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-conduct-and-certifications.pdf?la=en	
示例：云提供商行为准则 (CISPE)（2017 年 1 月）	https://cispe.cloud/code-of-conduct/	
示例：云提供商行为准则 (EU Cloud)（2018 年 11 月）	https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html	

相关 EPDP 第 1 阶段实施问题：无。

任务：

- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：8 月

j) 使用条款/披露协议/隐私政策

目标：围绕寻求访问非公开注册数据的第三方的使用条款制定政策要求：

- 为充分保护可提供给认证用户/第三方的个人数据，至少需要采取哪些必要措施？
- 应制定哪些数据访问程序？
- 为限制对正常访问数据的使用，应制定哪些程序？
- 是否需要为不同的用户组单独制定使用条款？
- 谁负责监控并强制遵守使用条款？
- 为要求遵守使用条款，将采用哪项机制？

相关思维导图问题：

P1-Charter-c
c1) 监管用户数据访问的规则/政策是什么？
c2) 一旦访问，监管用户数据使用的规则/政策又是什么？
c3) 谁负责制定和执行这些规则/政策？
c4) 如果用户滥用数据，将面临哪些制裁或处罚？
除适用法律规定的制裁以外，还包括未来对
数据遭到滥用的数据主体实施访问或赔偿限制。

TSG-Final-Q#4
详细说明只有特定类别的请求者可以下载活动日志，还是一般请求者均可下载活动日志。
TSG-Final-Q#10
描述向 CP 披露请求的条件（如果有）。
TSG-Final-Q#11
提供关于各系统组件的运营商责任的法律分析。
TSG-Final-Q#12
简要介绍提交不当披露投诉的程序及相应的可接受使用策略

需要审核的材料：

描述	链接	必读原因
持续访问完整 WHOIS 数据的可能统一访问模型框架 WHOIS 数据——使用条款在统一访问模型中的作用是什么？	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf 第 14-16 页	

相关 EPDP 第 1 阶段实施问题：

任务：

- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：9 月

k) 数据的保留与销毁

目标：为参与 SSAD 的各方保留的数据确定最低保留、删除和记录政策要求，包括但仅限于 gTLD 注册数据、用户帐户信息、交易日志和元数据（如请求日期和时间）

相关思维导图问题：

P1-Charter-c
c2) 一旦访问，监管用户数据使用的规则/政策又是什么？

TSG-Final-Q#5
描述对各系统组件施加的数据留存要求。

需要审核的材料：

描述	链接	必读原因
GDPR 第 5(1)(e) 条	https://gdpr.algolia.com/gdpr-article-5	
TSG 模型数据留存	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf，第 26 页	

相关 EPDP 第 1 阶段实施问题：建议 15：

1. 为针对第 2 阶段审议提供依据，EPDP 团队建议 ICANN 组织对所有活动流程和程序进行紧急审核，以便识别并记录从注册服务机构请求的个人数据超出“注册周期”期限的实例。随后，应识别、记录并依赖特定数据元素的留存期，为注册服务机构设置所需的相关特定最低预期数据留存期。EPDP 团队建议邀请社群成员参与数据收集工作，针对其他合法目的发表意见，为此可能需要适用不同的留存期。

2. 与此同时，EPDP 团队认识到，转移争议解决政策 (TDRP) 的最长合理留存期已设置为一年，因而建议注册服务机构在注册有效期后的 15 个月内，仅保留那些 TDRP 所必需的数据元素，并在此基础上增加 3 个月的数据删除时间，总计留存期为 18 个月。保留这项建议的依据是：TDRP 中有这样一项政策规定，即：根据该政策提出的投诉，只能在涉嫌违反转移政策（档案号：请参阅 TDRP 第 1.15 节）后的 12 个月内提出（档案号：请参阅 TDRP 第 2.2 节）。此留存期不会限制注册管理机构和注册服务机构出于建议 1 中指定的其他目的缩短建议 4-7 中提供的数据元素的留存期的权力。

3. EPDP 团队认识到，签约方可以根据本地法律或其他要求规定设置不同的留存期。EPDP 团队指出，这项建议或独立 ICANN 政策中的任何内容均未阻止签约方自行设置留存期，留存期可以比 ICANN 政策规定的时间长，也可以比 ICANN 政策规定的时间短。

4. 团队建议，ICANN 组织审核当前的数据留存弃权程序，提高效率、缩短请求响应时间及加强 GDPR 合规性。例如，如果某司法管辖区的注册服务机构成功获得了数据留存弃权，则同类注册服务机构可以通过通知程序申请相同的弃权，而不必单独提出申请。

任务：

- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：9 月

I) 财务可持续性

目标：确保 SSAD 的各个环节均获得可持续的财务支持。考虑如何以及由谁来承担 SSAD 实施和管理费用。

- 确定 2018 年 5 月之前是否存在市场效率低下的问题，同时确定 EPDP 第 1 阶段实施之后是否存在效率低下的问题。
- 即使为保障公共利益而披露注册数据，签约方和/或 ICANN 是否也应承担标准化解决方案的费用？
- 如果认证是可行解决方案，那么应收取相关申请费，还是根据披露类型（分级）、规模或数量确定收费结构？
- 是否应该（或可以）为数据主体披露数据做出补偿？

相关思维导图问题：无

需要审核的材料：

描述	链接	必读原因

相关 EPDP 第 1 阶段实施问题：无

任务：

- 确认关键术语定义
- 确定完整政策问题列表并分别审议
- 确定可能的解决方案或拟定建议（如果有）
- 确认章程中提出的所有问题均已得到解决和记录

目标完成日期：待定

附录 B——一般背景

流程和问题背景

2018 年 7 月 19 日，GNSO 理事会启动了快速政策制定流程 (EPDP)，并授权针对“临时规范”为 gTLD 注册数据团队制定 EPDP。与 GNSO PDP 不同的是，GNSO 理事会选择限制 EPDP 的成员构成，这是由于这项工作要在相对较短的时间内完成，并需要对资源进行合理分配。根据章程规定，GNSO 的各个利益相关方团体、政府咨询委员会 (GAC)、国家和地区名称支持组织 (ccNSO)、一般会员支持组织 (ALAC)、根服务器咨询委员会 (RSSAC)、安全性稳定性咨询委员会 (SSAC) 均受邀指定一定人数的成员和替补人员。此外，ICANN 董事会和 ICANN 组织也已受邀指定一定人数的联络人参与此项工作。前文提到的“诚招志愿者”的工作于 7 月启动，且 EPDP 团队于 2018 年 8 月 1 日召开了第 1 阶段的首次会议。

○ 问题背景

2018 年 5 月 17 日，ICANN 董事会通过了《gTLD 注册数据临时规范》。董事会现已采取措施制定临时要求，使得 ICANN 及其签约方能够继续遵守现有 ICANN 合规要求和社群制定的有关 WHOIS 的政策，同时遵守欧盟 (EU) 颁布的《通用数据保护条例 (General Data Protection Regulation, GDPR)》。这套《临时规范》根据《注册管理机构协议 (Registry Agreement, RA)》和《注册服务机构认证协议 (Registrar Accreditation Agreement, RAA)》中规定的临时政策流程而获得批准。《临时规范》获批后，董事会“应当立即执行 ICANN《章程》中确立的共识性政策制定流程”。[47]针对《临时规范》启动的共识性政策制定流程应需要在 1 年期内实施推行。此外，工作范畴中还包括：讨论设立一套非公开注册数据的标准化访问系统。

在 2018 年 7 月 19 日召开的会议中，通用名称支持组织 (GNSO) 理事会启动了《gTLD 注册数据临时规范》EPDP 并通过了 EPDP 团队章程。与 GNSO PDP 不同的是，GNSO 理事会选择限制 EPDP 的成员构成，这是由于这项工作要在相对较短的时间内完成，并需要对资源进行合理分配。根据章程规定，GNSO 的各个利益相关方团体、政府咨询委员会 (GAC)、国家和地区名称支持组织 (ccNSO)、一般会员支持组织 (ALAC)、根服务器咨询委员会 (RSSAC)、安全性稳定性咨询委员会 (SSAC) 均受邀指定一定人数的成员和替补人员。此外，ICANN 董事会和 ICANN 组织也已受邀指定一定人数的联络人参与此项工作。

[47] 请参阅《注册管理机构协议》第 3.1(a) 节：https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en

EPDP 团队还于 2018 年 11 月 21 日发布了第 1 阶段的《初步报告》，征询公众意见。EPDP 团队将公众意见纳入第 1 阶段最终报告，GNSO 理事会在 2019 年 3 月 4 日的会议上投票通过了 EPDP 第 1 阶段最终报告中的全部 29 项建议。2019 年 5 月 15 日，ICANN 董事会通过 EPDP 团队第 1 阶段最终报告，但以下两项建议未予采纳：1) 建议 1 的目的 2；以及 2) 建议 12 提出的删除“组织”字段数据的方案。根据 ICANN 章程，GNSO 理事会将与 ICANN 董事会开展协商，讨论 EPDP 第 1 阶段建议中未获得 ICANN 董事会采纳的部分。与此同时，实施审核小组 (IRT) 将实施 EPDP 团队第 1 阶段最终报告中已批准的建议。IRT 由 ICANN 组织 (ICANN org) 和 ICANN 社群成员共同组成。有关实施状态的更多详细信息，请参阅此处。

2019 年 5 月 2 日，EPDP 团队启动第 2 阶段工作。EPDP 第 2 阶段的工作范围包括：(i) 就非公开注册数据的标准化访问/披露系统进行讨论，(ii)《gTLD 注册数据临时规范》附录中指出的问题（即，“社群后续行动中的重要问题”），以及 (iii) 第 1 阶段悬而未决的问题，例如，法人与自然人，城市字段修订等。有关更多详情，请参阅此处。

附录 C——EPDP 团队成员和出席情况

EPDP 团队成员和出席情况

会议活动总结：

全体会议：

- 75 次全体会议，共计 155.5 小时
- 12 次面对面会议，共计 77.5 小时
- 01 次网络研讨会，共计 1.0 小时
- 总体出席率为 86%

小组会议

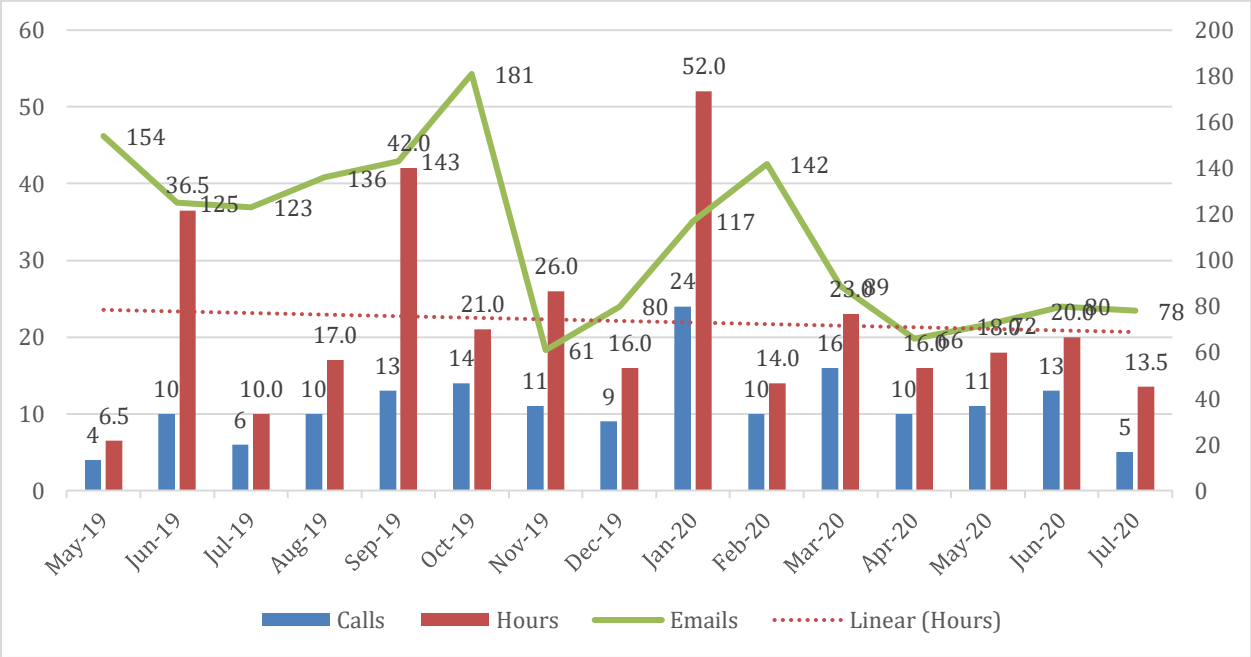
- 10 次次级小组会议，共计 18.0 小时

法务委员会会议：

- 19 次次级小组会议，共计 29.4 小时
- 01 次面对面会议，共计 1.5 小时

领导层会议：

- 48 次领导层会议，共计 47.5 小时
- 04 次领导层面对面会议，共计 20.5 小时



如需查看详细名单、SOI 和出席情况，请访问 https://community.icann.org/x/kBdIBg。

如需查看电子邮件存档，请访问 https://mm.icann.org/pipermail/gnso-epdp-team/。

全体会议 EPDP 团队积极成员（LC——服务于法务委员会）

成员类型/所属组织/姓名	SOI	起始日期	出席率	职责
当前参与者			87.9%	
成员				
一般会员咨询委员会			97.7%	
艾伦 • 格林伯格 (Alan Greenberg)	SOI	2019 年 4 月 3 日	97.7%	
海地亚 • 埃尔米尼亚维 (Hadia El-Miniawi)	SOI	2019 年 4 月 3 日	97.7%	LC
企业和商业用户选区			94.8%	
麦琪 • 米朗 (Margie Milam)	SOI	2019 年 4 月 3 日	95.4%	LC
马克 • 思凡卡瑞克 (Mark Svancarek)	SOI	2019 年 4 月 3 日	94.3%	
GNSO 理事会			98.3%	
拉菲克 • 丹马克 (Rafik Dammak)	SOI	2019 年 4 月 3 日	98.3%	主席
政府咨询委员会			93.6%	
克里斯 • 刘易斯 • 埃文斯 (Christopher Lewis-Evans)	SOI	2019 年 5 月 15 日	96.6%	
乔治亚斯 • 彻伦蒂斯 (Georgios Tselentis)	SOI	2019 年 4 月 3 日	88.5%	
劳伦 • 卡宾 (Laureen Kapin)	SOI	2019 年 10 月 21 日	96.1%	LC
ICANN 董事会			84.6%	
贝基 • 拜耳 (Becky Burr)	SOI	2019 年 9 月 9 日	93.5%	LC
克里斯 • 狄思潘 (Chris Disspain)	SOI	2019 年 4 月 3 日	78.2%	
知识产权选区			91.0%	
布莱恩 • 金 (Brian King)	SOI	2019 年 8 月 4 日	88.5%	LC
弗兰克 • 乔纳德 (Franck Journoud)	SOI	2019 年 1 月 12 日	95.7%	
互联网名称与数字地址分配机构			95.9%	
丹尼尔 • 哈罗兰 (Daniel Halloran)	-	2019 年 4 月 3 日	94.3%	
伊莉莎 • 阿格匹安 (Eleeza Agopian)	-	2019 年 12 月 6 日	98.4%	
互联网服务提供商和连接提供商选区			65.5%	
菲奥纳 • 阿颂嘉 (Fiona Asonga)	SOI	2019 年 4 月 3 日	44.8%	
托马斯 • 李凯尔特 (Thomas Rickert)	SOI	2019 年 4 月 3 日	86.2%	LC
非商业利益相关方团体			78.9%	
阿姆鲁 • 萨德尔 (Amr Elsadr)	SOI	2019 年 4 月 3 日	67.8%	
约翰（加尔夫） • 赫尔辛吉斯 (Johan (Julf) Helsingius)	SOI	2019 年 4 月 3 日	75.9%	
米尔顿.穆勒（Milton Mueller）	SOI	2019 年 4 月 3 日	81.4%	
史戴芬 • 菲利波维克 (Stefan Filipovic)	SOI	2019 年 5 月 21 日	84.5%	
丝黛芬妮 • 裴琳 (Stephanie Perrin)	SOI	2019 年 4 月 3 日	86.2%	LC
<空缺>	-			
注册服务机构利益相关方团体			85.0%	
詹姆斯 • 布雷德尔 (James Bladel)	SOI	2019 年 4 月 3 日	76.7%	
马特 • 瑟林 (Matt Serlin)	SOI	2019 年 4 月 3 日	86.2%	

福尔克尔 • 格莱曼 (Volker Greimann)	SOI	2019 年 4 月 16 日	92.0%	LC
注册管理机构利益相关方团体			90.0%	
艾伦 • 伍兹 (Alan Woods)	SOI	2019 年 4 月 3 日	90.8%	
马克 • 安德森 (Marc Anderson)	SOI	2019 年 4 月 3 日	95.4%	
马修 • 克罗斯曼 (Matthew Crossman)	SOI	2019 年 4 月 3 日	83.1%	LC
安全与稳定咨询委员会			92.1%	
本 • 巴特勒 (Ben Butler)	SOI	2019 年 4 月 3 日	93.1%	
塔拉 • 瓦伦 (Tara Whalen)	SOI	2019 年 5 月 15 日	90.9%	LC

全体会议 EPDP 团队积极候补人员：

成员类型/所属组织/姓名	SOI	起始日期	出席率	职责
候补人员				
一般会员咨询委员会				
巴斯蒂安 • 戈斯林 (Bastiaan Goslings)	SOI	2019 年 4 月 3 日	50.0%	
霍莉 • 雷谢 (Holly Raiche)	SOI	2019 年 4 月 3 日	33.3%	
企业和商业用户选区				
史蒂夫 • 德尔比安克 (Steve DelBianco)	SOI	2019 年 4 月 3 日	100.0%	
政府咨询委员会				
奥尔加 • 卡瓦利 (Olga Cavalli)	SOI	2019 年 5 月 22 日	95.6%	
拉胡尔 • 格萨恩 (Rahul Gosain)	SOI	2019 年 4 月 3 日	75.0%	
瑞恩 • 卡洛尔 (Ryan Carroll)	SOI	2019 年 12 月 18 日	100.0%	
互联网服务提供商和连接提供商选区				
休曼 • 拉尔 • 普拉丹 (Suman Lal Pradhan)	SOI	2019 年 4 月 3 日	33.3%	
非商业利益相关方团体				
戴维 • 凯克 (David Cake)	SOI	2019 年 4 月 3 日	90.0%	
塔蒂阿娜 • 托皮纳 (Tatiana Tropina)	SOI	2019 年 4 月 3 日	77.8%	LC
姚利 • 卡尔 • 奎罗斯 (Yawri Carr-Quiros)	SOI	2020 年 2 月 17 日	100.0%	
注册服务机构利益相关方团体				
欧文 • 斯米戈尔斯基 (Owen Smigelski)	SOI	2019 年 4 月 16 日	100%	
萨拉 • 怀尔德 (Sarah Wyld)	SOI	2019 年 4 月 3 日	98.7%	
蒂奥 • 葛茨 (Theo Geurts)	SOI	2019 年 4 月 3 日	80.0%	
注册管理机构利益相关方团体				
阿诺德 • 维特施恩 (Arnaud Wittersheim)	SOI	2019 年 4 月 3 日	80.0%	
贝斯 • 培根 (Beth Bacon)	SOI	2019 年 4 月 22 日	95.7%	
肖恩 • 伯塞里 (Sean Baseri)	SOI	2019 年 11 月 6 日	100.0%	
安全与稳定咨询委员会				
格雷格 • 亚伦 (Greg Aaron)	SOI	2019 年 10 月 5 日	77.8%	
罗德 • 拉斯穆森 (Rod Rasmussen)	SOI	2019 年 4 月 3 日	25.0%	

全体会议 EPDP 团队积极支持人员：

成员类型/所属组织/姓名	SOI	起始日期	出席率	职责
支持人员				
ICANN（互联网名称与数字地址分配机构）				
凯特琳 • 图伯根 (Kaitlin Tubergen)		2019 年 4 月 3 日		LC
马里卡 • 孔宁斯 (Marika Konings)		2019 年 4 月 3 日		
贝瑞 • 柯布 (Berry Cobb)		2019 年 4 月 3 日		LC
艾米 • 比文思 (Amy Bivins)		2019 年 6 月 3 日		LC
特里 • 阿纽 (Terri Agnew)		2019 年 4 月 3 日		
安德里亚 • 格朗东 (Andrea Glandon)		2019 年 4 月 3 日		
茱莉亚 • 毕思兰 (Julia Bisland)		2019 年 6 月 20 日		
米歇尔 • 代斯米特 (Michelle DeSmyter)		2019 年 6 月 20 日		
娜塔莉 • 蓓蕾格兰 (Nathalie Peregrine)		2019 年 4 月 3 日		

全体会议 EPDP 团队前参与者：

成员类型/所属组织/姓名	SOI	起始日期	出席率	职责	离开日期
前参与者	-				
成员	-				
GNSO 理事会	-				
亚尼斯 • 卡克林斯 (Janis Karklins)	SOI	2019 年 4 月 3 日	97.6%	主席	2020 年 7 月 3 日
政府咨询委员会	-				
阿什利.海内曼（Ashley Heineman）	SOI	2019 年 4 月 3 日	75.7%		2019 年 10 月 21 日
ICANN 董事会	-				
里昂 • 菲利普 • 桑切斯 • 安比亚 (Leon Felipe Sanchez Ambia)	SOI	2019 年 4 月 3 日	88.5%	LC	2019 年 9 月 9 日
知识产权选区	-				
亚力克斯 • 迪根 (Alex Deacon)	SOI	2019 年 4 月 3 日	87.5%		2019 年 12 月 1 日
互联网名称与数字地址分配机构	-				
常 • 努言 (Trang Nguyen)	-	2019 年 4 月 3 日	88.9%	LC	2019 年 4 月 10 日
非商业利益相关方团体	-				
艾顿 • 法比恩 • 弗德莱恩 (Ayden Fabien Férdeline)	SOI	2019 年 4 月 3 日	73.5%		2020 年 1 月 27 日
法赞内 • 巴蒂 (Farzaneh Badiei)	SOI	2019 年 4 月 3 日	69.2%		2020 年 1 月 27 日
注册管理机构利益相关方团体	-				
克里斯蒂娜 • 罗塞特 (Kristina Rosette)	SOI	2019 年 4 月 22 日	97.6%		2019 年 8 月 7 日
候补人员	-				
知识产权选区	-				
珍妮弗 • 戈尔 (Jennifer Gore)	SOI	2019 年 4 月 3 日	97.6%		2020 年 2 月 13 日

如需查看详细出席记录，请访问 https://community.icann.org/x/4opHBQ。

如需查看 EPDP 团队电子邮件存档，请访问 https://mm.icann.org/pipermail/gnso-epdp-team/。

附录 D——共识建议

以下是主席认定的 EPDP 团队最终报告中各项建议的共识级别。这些认定是根据此处所述的流程，采用 GNSO 工作组指南第 3.6 节“标准决策制定方法”及 EPDP 团队章程得出。

建议编号		主席拟定的共识级别	不支持建议或部分建议的工作组
1	认证	完全共识	
2	政府实体的认证	完全共识	
3	请求的标准与内容	完全共识	
4	回执	完全共识	
5	响应要求	大力支持，但存在严重异议	GAC（准确性） IPC BC
6	优先级	分歧	GAC（不支持 6.2） BC（不支持 6.2） IPC（不支持 6.2） ALAC（不支持 6.2） SSAC
7	请求者目的	达成共识	NCSG（有条件地删除脚注）
8	签约方授权	大力支持，但存在严重异议	GAC（准确性，反对 8.17） IPC BC
9	SSAD 处理自动化	大力支持，但存在严重异议	IPC BC ALAC
10	确定 SSAD 响应时间的可变 SLA	大力支持，但存在严重异议	RrSG（不支持紧急请求 SLA） SSAC IPC BC
11	SSAD 条款和条件	完全共识	
12	披露要求	大力支持，但存在严重异议	GAC（准确性） SSAC
13	查询策略	完全共识	
14	财务可持续性	分歧	ALAC

			GAC SSAC IPC BC
15	日志记录	完全共识	
16	审计	完全共识	
17	报告要求	完全共识	
18	成立 GNSO 常任委员会，审核关于 SSAD 的政策建议的实施情况	大力支持，但存在严重异议	ALAC BC IPC GAC
19	信息显示：附属隐私/代理提供商	完全共识	
20	城市字段	达成共识	NCSG
21	数据留存	完全共识	
22	目的 2	达成共识	NCSG

附录 E——少数派声明

一般会员咨询委员会 (ALAC)
企业选区 (BC)/知识产权选区 (IPC)
政府咨询委员会 (GAC)
非商业利益相关方团体 (NCSG)
注册服务机构利益相关方团体 (RrSG)
注册管理机构利益相关方团体 (RySG)
安全与稳定咨询委员会 (SSAC)

ZH

AL-ALAC-ST-0720-04-01-ZH
初始语言：英语
日期：2020 年 7 月 29 日
状态：已批准

一般会员咨询委员会

ALAC 关于快速政策制定流程 (EPDP) 的声明

提交纳入快速政策制定流程 (EPDP)《gTLD 注册数据临时规范》第 2 阶段最终报告的 ALAC 声明

ALAC 参与处理 EPDP 事务并做出以下声明：

1. ALAC 认为 EPDP 必须成功并将为此努力。
2. 我们正在组建支持团队，确保广大社群成员理解本文档介绍的内容、收集意见并获得支持。
3. ALAC 认为，个人注册人也是用户，我们会定期代表用户开展工作（如同域名到期后根据 PDP 发起行动保护注册人权利一样），如果注册人的需求不同于 40 亿非注册人互联网用户，则以后者的需求为准。我们认为 GDPR 和本 EPDP 就是这种情况。
4. 尽管部分互联网用户会咨询 WHOIS，但在某些情况下无法获得这项支持，我们的主要工作焦点在于确保用户在互联网环境中安全无虞。这意味着，执法机构、网络安全研究人员、域名欺诈专家及其他人员将共同保护用户免受网络钓鱼、恶意软件、垃圾邮件、欺诈、DDoS 攻击的侵害，期间可尽量减少 WHOIS 数据访问以增强效果。当然，所有相关行为均需符合 GDPR 限制。

我们积极开展工作，支持 EPDP 流程，目前代表近 50 亿互联网用户行事。

EPDP 第 2 阶段的目标是开发所谓的非公开注册数据标准化访问/披露系统 (SSAD)，以及解决 EPDP 第 1 阶段未能完全解决的众多问题。

我们已经完成大量工作，但 ALAC 认为，如果部署 SSAD，达成支持社群所要求的目标的可能性将很小。这些社群需要访问具体、准确而又可用的非公开数据，而且需要采用可预测的方式及时进行访问。

实现这一目标的主要方法如下：

- 切勿扩大隐私立法范围。仅编辑受相关法律保护的数据；
- 确保数据准确且联系信息可用——这是提供联系信息的唯一理由；

- 在可能的合法范围内，自动处理查询，以便快速做出响应（如有可能，将接近瞬时）

遗憾的是，最终报告未做出任何确定性响应。

具体要点：

- 第 1 阶段允许对法人（公司）及自然人（个人）信息进行编辑，而且大多数注册服务机构和注册管理机构都在全面编辑相关信息。另外，无论身处何地，都可以进行编辑。
- 原定于第 2 阶段彻底解决法人与自然人的问题；但是，尽管开展了一些讨论，但问题仍被返回 GNSO 理事会，以便日后加以解决。
- GDPR 要求在处理数据时保持目的准确。对于 RDS 数据，意味着了解注册人身份并促进联系。WHOIS 准确性研究表明，过去公开获取信息时，信息并不准确。原定于第 2 阶段全面讨论与目前编辑的数据有关的准确性问题。不过，这项工作仍未完成。GNSO 理事会指示 PDP 暂时搁置此主题，目前解决方法尚不明朗，GNSO 理事会考虑日后再做解决。
- 研究发现，目前与注册人联系采取的方法（主要是 Web 表单）不够有效，而且并未向发件人反馈可能抵达注册人的消息范围。现已责令 GNSO 理事会进一步讨论，以便日后加以解决。
- SSAD 将自动对一些用例做出响应。目的是随着法律、法学和合同问题的发展，在“演进”机制的辅助下采用自动化方式处理更多用例。根据演进机制建议：要求 GNSO 常任委员会 (SC) 负责对新用例进行审批，不仅包括签约方（如果处理不当，可能会遭受处罚），也包括 GNSO 理事会。允许 SC 提出纯粹的实施（需获得 GNSO 理事会批准方可实施）和政策（需制定 GNSO 政策流程（如 PDP）方可继续执行）建议。目前尚未确定是将新的 SSAD 决策用例建议视为实施方案，还是必须制定新的 PDP（或等效方案）以切实自动处理相关用例（未来可能会增加新的用例）。

  尽管有代表对此持有较强保留意见，ALAC 和其他几个团体接受当前的 SSAD 模型，因为我们确信演进机制可以务实而又及时地做出更改。鉴于法律和责任问题，虽无法保证做出此类更改，但存在这种可能性。基于目前对演进机制的认识，尚未最终确定 GNSO 理事会运作机制及 GNSO 理事会建议处理机制，ALAC 绝不会同意当前的 SSAD 模型。

此外，尽管默认情况下，常任委员会建议书要求 GNSO 理事会以标准多数票通过决议，但有可能改为要求绝对多数票通过决议[48]。

- 财务模型有些麻烦。乍一看，由 SSAD 用户承担大部分运营成本似乎没有什么不合理，但在确定价格时会试图设置较高费用以阻止使用。这不仅会致使财务目标难以实现，还将导致整项工作无效。定价必须灵活，确保 SSAD 切实发挥效用。为此，目前尚不清楚 ICANN 可能需要在多大程度上提供服务补贴。

所有这些问题皆因以下缘由未予解决：明确指示暂不解决 EPDP 问题；选择暂不解决问题；建议措词含糊不清，因而对结果信心不足。

GNSO 理事会在审议本最终报告时，可以适当解决所有这些问题。

因此，ALAC 有条件地支持本报告，但须遵循下列 GNSO 理事会行动。

如果无法实现这些成果，则 ALAC 认为本报告将演变为多年实施计划，因而导致出票系统受到过分追捧，但实际上过于复杂且非常昂贵。因此，最终报告并未获得我们的全部支持，但建议 19-22 除外[49]。

GNSO 理事会为确保 ALAC 支持 EPDP 最终报告需要取得的成果：

1. GNSO 理事会同意，演进常任委员会就其他 SSAD 决策用例提出的建议（完全符合 EPDP 政策建议 9.3）将被视为“实施方案”，无需进一步政策审议。
2. 法人与自然人、准确性、WHOIS 准确度报告体系和匿名联系人电子邮件问题将得到充分解决，届时 ICANN 咨询委员会将根据需要全面参与讨论的各个环节。如果认定此类问题属于政策问题，则必须委派有权提出政策建议的工作组解决问题，并指派一名资深的无冲突主席领导工作组。GAC、ALAC 和 SSAC 必须参与制定工作组要求或章程。目标是在 2021 年 4 月之前完成所有工作。
3. GNSO 理事会同意，只需按照 GNSO 政策手册的当前要求获得 GNSO 多数票通过即可批准演进常任委员会建议。
4. GNSO 理事会确认，实施阶段进行定价审议时，必须邀请 SSAD 潜在用户参与其中，不仅要考虑成本回收，还要考虑 SSAD 用户支付定价的实际能力和意愿。

2020 年 7 月 29 日经 ALAC 一致批准
艾伦 格林伯格 (Alan Greenberg) 代表 ALAC 提交

[48]绝对多数票允许一个利益相关方团体外加一家机构的一名成员否决任意 GNSO 行动。
[49]为避免存疑，如果未达到条件，ALAC 仍将支持建议 19-22，但不支持报告的其余部分。

EPDP 第 2 阶段最终报告 ALAC 少数派声明附录

一般会员咨询委员会 (ALAC) 成员感谢提供机会提交 2020 年 7 月 29 日提交的声明附录。

ALAC 及其 EPDP 团队现在可以趁机审核并讨论 BC/IPC、GAC 和 SSAC 提交的声明以及其他 EPDP 成员组提交的声明。

尽管 ALAC、BC、IPC、GAC 和 SSAC 在处理报告立场时采取的方法各不相同，但 ALAC 在总体上赞同 GAC SSAC 和 BC/IPC 声明中提出的立场。特别是，ALAC 感谢 GAC、SSAC 和 BC/IPC 提供的深入而富有见地的分析。

鉴于经过一年多颇具挑战性的辩论得出的结果仍存有分歧，ALAC 对此并未掉以轻心。显然，这种情况并非暗示的那样简单，我们存在分歧是因为“我们还没有如愿以偿”。如果在解决经认定对 SSAD 成功至关重要的问题之前贸然行动，将导致系统无法满足 SSAD 用户的需求，而且几乎没有机会显著纠正这些问题。我们希望 GNSO 和董事会（如适用）在流程推进过程中进行深入考量。

ALAC 已于 2020 年 8 月 24 日批准。

企业选区 (BC) 和知识产权选区 (IPC) 关于 EPDP 团队第 2 阶段最终报告的少数派声明

EPDP 第 2 阶段最终报告未能提供可满足用户需求的标准化访问系统。因此，企业选区 (BC) 和知识产权选区 (IPC) 必须对此提出异议。

正如我们在针对 EPDP 第 1 阶段最终报告的声明中所指出的那样，BC 和 IPC 是 ICANN 自下而上的、基于共识的多利益相关方模型的坚定支持者，我们积极认真地参与 EPDP 相关工作就是很好的证明。EPDP 第 2 阶段旨在创建一个标准化系统以实现以下双重目标：一是保护注册人的个人数据；二是在用户出于合法目的需要合法处理注册人数据时，为用户提供一致、及时和可预测的访问权限。由于第 2 阶段最终报告未能实现上述目标，所以我们认为这份报告是不可接受的。

共同关心的问题

IPC 和 BC 支持对个人数据进行隐私保护，并且隐私法也致力于在个人隐私权与其他合法利益之间找到一个平衡点。遗憾的是，第 2 阶段最终报告未能实现这一平衡。这一失误对那些努力保护自己的基本权利，以及那些维护公共利益或其他合法利益的人造成了伤害。BC 成员所关注的问题包括增强用户对在线通信和商业互动的信心（正如欧盟 NIS 指令所提出的那样）。IPC 成员所关注的问题包括：保护消费者免遭网络钓鱼、危险假冒产品和其他欺诈（欧盟基本权利宪章第 38 条的规定）的威胁，以及保护知识产权（欧盟基本权利宪章第 17 条第 2 节的规定）。

IPC 和 BC 指出，第 2 阶段最终报告未能解决欧盟委员会和比利时数据保护机构 (DPA) 以及 ICANN 自己的三个咨询委员会提出的若干问题，这三个咨询委员会包括：代表执法机构和消费者权益保护利益的政府咨询委员会 (GAC)、代表互联网最终用户利益的一般会员咨询委员会 (ALAC)，以及负责就与互联网名称和地址分配系统的安全性和完整性相关事宜向 ICANN 董事会提供建议的安全与稳定咨询委员会 (SSAC)。

欧盟委员会和比利时 DPA 共同关心的问题

欧盟委员会[50] 敦促 *“ICANN 与社群一起，共同开发一个适用于所有注册管理机构和注册服务机构的统一访问模型，并按照《通用数据保护条例》(GDPR) 的规定，提供一种稳定、可预测并且切实可行的方法，供具有合法权益或持有其他合法理由的用户访问非公开的 gTLD 注册数据。”* 欧盟委员会表示，其认为这项工作 *“至关重要且非常紧迫”*，并敦促 ICANN *“在尽可能最短的时间范围内开发并实施一*

[50]请参阅：https://www.icann.org/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf

套切实可行的访问模型……”。比利时 DPA 是 ICANN 设立在比利时的监督机构，它认为这套集中式模型“*在安全性方面对于数据主体而言是一个更好的‘常识性’选择*”。[51]遗憾的是，第 2 阶段最终报告根本没有提供访问方法，更没有提供某种可被描述为“*稳定、可预测且切实可行的*”方法了。恰恰相反，第 2 阶段最终报告仅提供了一个提交请求的中心位置。这种做法表明它拒绝遵循比利时 DPA 的指导方针，赞成由 2000 多个独立的签约方自行决定是否公开数据，而根据 ICANN 的合同或政策，这些签约方都不需要聘请法律顾问、数据保护主管或隐私专业人员。

GAC 与 BC 和 IPC 共同关心的问题

对于 EPDP 团队未能解决数据准确性以及如何区分自然人和法人的问题，我们也与 GAC 有着同样的担忧。GAC 在其 6 月 22 日致 GNSO 理事会的信函中[52]指出“*这些问题关乎公共利益。当前 EPDP 工作阶段不妥善解决这些问题，就有可能形成一个缺少提高公共安全的重要功能的不完整系统。而且，未能解决这些重要问题会使人们质疑 GNSO 政策制定流程在解决对非 GNSO 利益相关方和公共利益具有重要意义的问题方面的合法性和有效性。*”遗憾的是，GAC 的请求在第 2 阶段被忽略了。尽管 GDPR 要求确保数据准确性，但是 GNSO 理事会从 EPDP 第 2 阶段工作的职权范围中移除了准确性相关工作，并且第 2 阶段最终报告也没有妥善解决区分自然人和法人注册人的问题。

SSAC 和 ALAC 与 BC 和 IPC 共同关心的问题

关于 EPDP 第 1 阶段初步报告的 SSAC 意见 (SSAC 111)[53] 引发了许多担忧，人们担心这些建议可能“*远远达不到 SSAC 所认为的在 ICANN 职权范围内能够和可能解决安全性和稳定性问题*”。同样，在其 2020 年 5 月 5 日关于初步报告附录的声明中，ALAC 也对未能解决关于如何区分自然人和法人注册人以及准确性等问题表示关切[54]。

EPDP 第 2 阶段最终报告的实质性问题

除了之前 GAC、ALAC 和 SSAC 提出的担忧之外，第 2 阶段最终报告中的以下问题也使 BC 和 IPC 对此份报告提出异议。

- ***缺乏集中披露且演进机制不足***。在第 1 阶段之后，我们希望制定一项支持集中制定决策的政策。分散式决策固有的低效率和不一致性显而易见，具

[51]请参阅：https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[52]请参阅：https://gac.icann.org/advice/correspondence/outgoing/GAC%20Chair%20letter%20to%20GNSO%20Council%20Chair%20-%20Next%20Steps%20on%20Key%20Policy%20Issues%20not%20Addressed%20in%20EPDP%20Phase%202.pdf
[53]请参阅：https://www.icann.org/en/system/files/files/sac-111-en.pdf
[54]请参阅：https://atlarge.icann.org/advice_statements/13775

体体现在：签约方负担的成本较高，披露请求的处理速度较慢，以及由于每个签约方对每个请求都应用自己的主观判断，因此，请求方与披露方之间发生争议的可能性较大。

尽管如此，为了找到折中解决方案，我们同意考虑（但没有接受）所提议的*混合模型*，即，初步的披露决定基本上采用手动的分散式处理，但将会根据在 SSAD 实施过程中获得的经验，以及在法律方面不断明确 GDPR 解释要求，演变为自动化的集中式处理。

我们预计，随着时间的推移，在适当的保障措施下，该系统将会为拥有合法身份且经过认证的请求者提供出于合法目的对所请求的注册人数据的访问权限。例如，持有伪造销售或侵犯版权的合理证据且经过认证的请求者，如果伪造销售或侵犯版权行为确认属实，则应快速且可预测地收到相关域名的注册人数据。这样一个清晰、一致且可扩展的系统，将因公众始终可以访问注册人数据而极大地提高 DNS 系统的信任度和问责制，但是第 2 阶段最终报告却并没有提供这样的内容。

第 2 阶段最终报告并没有促使 ICANN 演变成为集中决策者的自然角色。相反，最终报告却赋予签约方过度的酌情处理权，使他们能够单独解释根据 GDPR 和他们与 ICANN 签署的合同所承担的责任和义务，而没有任何合理性、一致性或其他保障措施方面的要求。最终报告也没有提供一个充分的机制，以允许未来采用自动化的集中处理方式。这样做的后果是会永久性地陷入分散式决策的低效率境况，例如，导致 SLA 不合理地延长，即便是与对生命或关键基础设施迫在眉睫的威胁有关的紧急请求也是如此。（第 9 项和第 18 项建议）

- ***<u>未能区分自然人和法人</u>***。第 2 阶段最终报告赋予签约方自主全权决定是否区分自然人和法人，因此没有提供关于 GDPR 未涵盖的*法人*如何访问注册人数据的明确说明。EPDP 团队寻求并获得了 Bird & Bird （EPDP 聘请的外部法律顾问）的法律意见，后者就 GDPR 关于如何区分自然人和法人注册人的法律义务提供了指导。但是在 IPC、BC、GAC、SSAC 和 ALAC 多方的反对声中，EPDP 团队没有对这个问题进行讨论。GDPR 并不要求对法人的联系人数据进行持续的批量修改[55]，因为这样会削弱 DNS 的信任度、问责制和透明度。因此，这是 EPDP 团队的一个不可接受的失误。（第 8 项建议）

[55] AFNIC 提交的关于 EPDP 第 2 阶段报告附录的意见支持这一观点。“*我们对提议不区分自然人和法人注册的做法表示担心。正如许多评论者所指出的那样，我们认为这是过度应用 GDPR 的做法。尽管 GDPR 不保护与法人有关的数据，但我们还是要提醒 ICANN 注意 2017 年 12 月 11 日的信函中第 29 条数据保护工作组提出的意见*

- ***未能解决数据准确性问题***。尽管目前有足够的工具来验证注册人数据的准确性，但是第 2 阶段最终报告未能按 EPDP 在第 1 阶段所商定的那样解决注册人数据准确性这个基本问题。WHOIS 数据不准确是 20 多年来一直存在的问题。EPDP 团队没有遵循其请求获取的关于解释 GDPR 准确性要求的法律咨询意见。EPDP 团队也没有遵循欧盟委员会的建议，他们的建议确认数据准确性不仅仅只符合数据主体的利益。明显虚假的数据不受数据隐私法的保护，而保留域名系统中虚假或虚构注册人数据的批量修改则代表 EPDP 的另一个失误，这进一步削弱了 DNS 的信任度、问责制和透明度。（结论 2）

- ***执法政策不足***。第 2 阶段最终报告缺乏要求签约方根据合法请求提供数据的合同责任。如上所述，第 2 阶段最终报告未能充分提供一个客观依据或是一个可预测且可扩展的一致程序，以便拥有合法依据和合法目的的经过认证的用户在请求使用数据时，可以获取准确的注册人数据，包括最初本来不该隐藏的数据。第 2 阶段最终报告未能赋予 ICANN 强制遵守最终报告中提出的薄弱建议的权力。如果缺乏确保遵守共识性政策的机制，那么分散式 SSAD 就没有多大价值。遗憾的是，这份报告仅考虑了强制执行程序要求，却没有赋予 ICANN 合规部审核不当拒绝合法请求的权力。这不仅削弱了整个政策，而且使其失去了法律效力。（第 5 项和第 8 项建议）

总之，结果就是第 2 阶段最终报告提出的一套系统和多项政策，整体上不足以满足商定的 SSAD 既定目标，包括其用户的需求。因此，第 2 阶段最终报告无法维护 DNS 的信任度、安全性和弹性。

在制定这项政策时，至关重要的一点是 ICANN 社群为解决日益严重的域名滥用问题提供支持，因为滥用问题对 DNS 的安全、稳定与弹性，以及更广泛的互联网生态系统（包括最终用户的安全）造成了威胁。最近，签约方 Neustar 在有关由于新冠肺炎 (COVID-19) 疫情导致互联网流量总体增长，以及随之而来的网络攻击问题的报告中指出：“*Neustar 预计流量会增加，但我们也看到，使用我们测量的几乎每一个衡量标准的攻击都出现了急剧增加。我们观察到，不仅整体攻击数量有所增长，而且攻击严重程度也有所增加……*”[56]除了指出“*与 2019 年第一季度相比，2020 年第一季度的攻击数量增加了两倍多*”之外，Neustar 还报告说：“*DNS 劫持有所增加，在这种攻击伎俩中，DNS 设置会将用户重定向到一个表面上看起来相同但通常包含伪装成有用内容的恶意软件的网站。*”

共识性方面的结果

IPC 和 BC 提醒 GNSO 理事会和 ICANN 董事会，EPDP 第 2 阶段最终报告应制定关于单一**系统**（即 SSAD）的政策。虽然共识会议应针对逐条建议进行讨论，但由于所

[56]请参阅：https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report

有建议都对 SSAD 整体产生影响，因此，它们在本质上是相互关联和相互联系的。因此，应在系统级别全面考虑，而不是严格按照每项建议单独考虑共识会议的结果。

建议编号	
1 认证	支持
2 政府实体的认证	支持
3 请求的标准与内容	支持
4 回执	支持
5 响应要求	反对
6 优先级	反对
7 申请人目的	支持
8 签约方授权	反对
9 SSAD 处理自动化	反对
10 确定 SSAD 响应时间的可变 SLA	反对
11 SSAD 条款和条件	支持
12 披露要求	支持
13 查询政策	支持
14 财务可持续性	反对
15 日志记录	支持
16 审计	支持
17 报告要求	支持
18 通过 GNSO 常任委员会来审核关于 SSAD 的政策建议的执行情况	反对
19 显示附属隐私/代理提供商的信息	支持
20 城市字段	支持
21 数据留存	支持
22 目的 2	支持

除此之外，IPC 和 BC 还反对以下非建议性章节中的措辞：

- 第 1.2 节和第 2.3 节（关于“未解决的事项”的描述）。我们不支持对法人和自然人结果的描述。
- 第 3.1 节（关于如何得到“混合”模型的描述）。 我们接受采用混合模型这个提议的条件是，能否使用支持这种转变的演进机制来逐步转向采用 CGM 集中式决策。
- 结论——准确性（第 60 页）。

评估对请求者的总体价值

虽然 EPDP 第 2 阶段团队花费了大量时间和精力分析 SSAD 自身的财务可持续性，但是我们认为从用户（即，寻求披露注册人数据的系统用户）的角度分析成本和收益同样重要。这样做至关重要，因为第 2 阶段的政策要求请求者为 SSAD 的持续运营和维护支付大部分（如果不是全部）的费用，因此，我们预计请求者需要支付的认证费和请求处理费将会很高。

而且，目前制定的 SSAD 政策将会对一直以来比较依赖 WHOIS 数据的人员产生超出直接成本之外的其他重大影响。这些间接成本与以下各项因素有关：

- **未及时响应**：由于上述诸多问题，对披露请求的响应时间将会不合理地延长，进而影响到与调查和管理滥用问题及非法问题有关的程序的效率。
- **不完整**：由于不能再执行所谓的“反向”解析，现在更难识别与事件或攻击相关联的所有域。
- **无法归因**：抑制反向解析会干扰在有效的响应时段内（如果有）将犯罪或滥用活动归因于注册人（参与者）的能力。请求者，尤其是网络攻击的第一响应者，将在更大程度上依赖邻近因素而不是归因模型来部署对策或缓解攻击。
- **不准确**：不能保证返回的数据是准确的，也没有规定由独立方审核注册数据的准确性。请求者承担了数据披露请求的成本，但却无法明确知晓响应的效用或价值。
- **未遏制**：无法及时、完整地列举与犯罪或滥用活动相关的域，会延误针对网络攻击采取初步应急措施的时机。因此，攻击持续时间将超出历来确立的 1-4 小时缓解这个目标。当前定义的 SLA 不足以解决以下问题：网络钓鱼（其生命周期为数小时而不是数天），或恶意软件攻击（会给受害者造成严重的直接成本或损失）。
- **不可预测性**：分散的分布式披露模型将会导致不可预测且不可靠的访问和披露系统。这会阻碍请求者从多个签约方寻求披露数据的努力，导致无法获取与单个网络犯罪或滥用活动相关的大量域名信息。

我们一直知道，使用 SSAD 需要支付认证费。然而，很明显第 2 阶段最终报告界定的 SSAD 的价值和优势根本不足以证明使用 SSAD 的费用（直接和间接）是物有所值的。

结论

ICANN 董事会在 2018 年 5 月采纳《临时规范》时曾指出，“*董事会的这项措施预计将会对 DNS 的持续安全、稳定或弹性产生直接影响，因为在社群致力于制定共识性政策的过程中，这项措施将最大程度地协助维护 WHOIS 系统。*”[57]在 2019 年 11 月召开的 ICANN 第 66 届蒙特利尔会议期间，ICANN 董事会和首席执行官在公开论坛上重申了对注册人数据进行可扩展访问的重要性，以确保互联网及其用户安全。EPDP 团队两年多紧张工作的成果只不过是对 [前期 EPDP] 现状进行了认定：出于合法的公共利益和私人利益的个人和实体，基本上无法访问用于识别域名所有者和用户所需的 WHOIS 数据元素。

出于上述原因，ICANN 董事会批准的使命和目的迫使我们对第 2 阶段最终报告中提出的政策建议提出异议。

尽管 IPC 和 BC 出于一番好意，但 EPDP 的尝试却失败了。事实证明，EPDP 团队无法处理 GDPR 引发的纯粹法律问题。监管者和立法者应该注意到，ICANN 多利益相关方模型已经不能满足消费者保护、网络安全和执法的需要。因此，不仅需要获得关于 GDPR 的明确监管指导，而且还需要寻找替代的法律和监管办法。

关于 BC 和 IPC

经 ICANN 董事会批准的商业和企业用户选区 (BC) 的使命是“*确保 ICANN 在履行其职能时可问责和保持透明，以及 ICANN 政策立场与互联网的发展保持一致，即，能够增强用户对在线通信和商业互动的信心……*”

正如 ICANN 董事会所批准的那样，知识产权选区 (IPC) 的宗旨是“*代表全球知识产权所有者的观点和利益，特别注重商标、版权和相关知识产权及其对域名系统 (DNS) 的影响和相互作用，并确保这些观点（包括少数人的观点）如实地反映在 GNSO 理事会向 ICANN 董事会提交的建议中。*”

[57]请参阅：https://www.icann.org/resources/board-material/resolutions-2018-05-17-en

政府咨询委员会关于 gTLD 注册数据 EPDP 团队第 2 阶段最终报告的少数派声明

注：*一般会员咨询委员会 (ALAC)、企业选区 (BC) 和知识产权选区 (IPC) 支持以下意见中表达的观点。*

简介

GAC 真诚地感谢整个 EPDP 团队、敬业的 EPDP 主席以及 ICANN 支持人员在过去 23 个月中所付出的辛勤努力，感谢他们花费大量时间和精力来制定这些关于访问和披露域名注册数据（以前称为 WHOIS）的复杂而重要的政策建议。《ICANN 章程》承认，WHOIS 数据是满足“合法的执法需要”以及“促进消费者信任”不可或缺的要素。[58]GAC 也一再重申这些重要目的，指出 WHOIS 数据用于大量合法活动，包括：协助执法机关进行调查，协助企业打击欺诈行为和滥用知识产权，维护公共利益，以及增强用户对互联网作为可靠的信息和通信手段的信心。[59]

认识到这些重要目的，ICANN 制定的《gTLD 注册数据临时规范》旨在“最大程度地确保 WHOIS 的持续可用性，同时维护互联网唯一标识符系统的安全性和稳定性。”[60]“最终建议”包含一些有用的元素，这些元素是对管理域名注册数据访问的现有《临时规范》的改进。然而，GAC 必须拒绝支持某些建议，因为这些建议以其目前的形式无法在以下两方面之间取得适当的平衡：保护向注册管理机构和注册服务机构提供数据的人的合法权利，以及保护公众免遭试图利用域名系统的恶意分子带来的伤害。[61]在这方面，GAC 着重指出域名系统是一种全球性公共资源，必须满足其所有用户（包括消费者、企业、注册人和政府）的需求。

在这份少数派声明中，GAC 就有关最终建议实施方式的公共政策问题提出了自己的意见：

1) 目前的结论是采用分散式，而不是集中式披露系统，
2) 目前不包含用于审核披露决定的强制性标准，
3) 没有充分解决消费者保护和消费者信任问题；
4) 目前没有可靠的标准化访问/披露系统 (SSAD) 演进机制，以满足不断增加的法律澄清要求；以及
5) 可能会施加财务要求，使 SSAD 面临为其用户（包括那些检测到网络安全威胁并采取应对措施的用户）支付不成比例的成本的风险。

[58] 《ICANN 章程》注册目录服务审核 § 4.6(e)。
[59] *例如，请参阅*《GAC 阿布扎比公报》第 VII.3 节第 11 段，以及 2007 年关于 WHOIS 服务的 GAC 原则。
[60] *请参阅 ICANN 数据保护/隐私问题*网页：https://www.icann.org/dataprotectionprivacy
[61] GAC 及其他利益相关方团体反对以下建议：5 - 响应要求；6 - 优先级；8 - 签约方授权；14 - 财务可持续性；18 - 通过 GNSO 常任委员会来审核关于 SSAD 的政策建议的执行情况。*请参阅* EPDP 第 2 阶段最终报告附录 D 中“共识性方面的结果”部分。

此外，正如我们在关于 EPDP 第 2 阶段初步报告附录的 GAC 意见中着重强调的那样，第 2 阶段最终报告目前没有解决某些关键问题（最突出的是数据准确性、对根据 GDPR 不受保护的法律实体屏蔽数据，以及使用匿名电子邮件）。此外，该模型的优势还在于能够进一步澄清每个数据控制人和处理人的地位和作用。GAC 要求 GNSO 理事会确保这些重要问题在 EPDP 的下一个工作阶段（最后的第 3 阶段）得到及时解决。

分散的披露系统

虽然“最终建议”提供了一个用于提交请求的集中式系统，但在数据披露方面却缺乏这种集中处理方式。目前的建议是创建一个分散的系统，这可能会导致无法充分访问注册数据，并可能延误执法、知识产权保护和网络安全调查的进度。GAC 警告不要创建“根据所涉及的注册服务机构可能由数千个不同策略组成的分散式访问系统”，并指出“缺乏一致的非公开信息访问策略可能会导致延误”，进而妨碍调查并可能放任潜在的有害行为继续损害公众利益。[62]GAC 认为，这一结果不符合 GAC 对“稳定、可预测且切实可行的非公开 WHOIS 信息的访问机制”的预期。[63]值得注意的是，比利时数据保护机构认可集中式模型的潜在优势，并明确承认 GDPR 不禁止披露模型中各种功能的自动化。[64]

尽管如此，披露建议：

- 几乎完全依赖于 2000 多个 ICANN 认证注册服务机构的自行评估和决定；[65]
- 没有充分解决自动化如何发挥作用的问题，只提供了两种自动化响应方式；[66]以及
- 没有建立可靠的机制来扩大自动披露请求的类别，以响应未来的法律指导或者甚至适用的隐私法的变更。[67]

现有的分散式披露系统，加上考虑和建议未来采用集中式系统的相对不确定的时间框架，这些因素都可能会影响 SSAD 的稳定性和可预测性。

[62] 《GAC 巴塞罗那公报》（第 IV.2 节“其他问题 – 参考《临时规范》”，第 6 段）。
[63]《GAC 巴拿马公报》，请参阅“GAC 向 ICANN 董事会提出的共识性建议的理由依据”（第 V.1 节，第 7 段）
[64] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[65]第 8 项建议
[66]第 9.41 项和第 9.42 项建议
[67] Rec.8.17 and 18

缺乏用于审核披露决定的强制性标准

GAC 承认，根据适用的数据保护法规（包括 GDPR 在内），签约方仍将负责决定是否披露域名注册数据，并且可能需要承担与该决定相关的某些责任风险。对于签约方据此积极寻求保持对是否披露域名注册数据的决定的控制权这种做法，GAC 虽然表示理解，但同时也指出，这些关于是否披露数据的分散式决定，很大程度上会免受 ICANN 合规部的质疑和执法行动。[68]

注册数据对 DNS 的安全性和稳定性至关重要，人们真的担心签约方在处理请求者获取公共数据的请求时，可能会无意或有意地对公共利益做出不适当的权衡。ICANN 首席执行官最近向欧洲数据保护理事会表达了这种担忧，并指出“由于缺乏法律确定性，注册服务机构作为数据控制人可能会以绝对方式评估数据隐私和数据保护，而不考虑其他权利和合法利益，以避免可能的监管制裁或针对其行为的判决。”[69]拒绝访问域名注册数据的合法请求会产生切实的后果。GAC 在其《巴塞罗纳公报》中指出，调查和研究表明，针对 GDPR 实施的《临时规范》对执法机构和网络安全专业人员产生了负面影响，使他们无法利用曾在 WHOIS 系统中公开可用的信息来调查和缓解犯罪行为。[70]

现有的建议没有提供审查披露决定的机制。现阶段的拟议系统不包含 ICANN 合规部在对披露决定中存在的实质性问题进行审核方面所发挥的作用的规定。相反，ICANN 合规部在审核有关未能遵守*程序性*要求或系统滥用的投诉问题方面发挥着有限的作用。[71]因此，SSAD 一方面建议开发一套系统（可能会鼓励采取保守的披露决定方法来降低责任风险），但另一方面却没有在 ICANN 的执行机制中充分提供对披露决定的有力审核。授予签约方审核披露请求的完全自主决定权，可能会削弱 ICANN 确保域名注册数据持续可用性的职责。域名注册数据作为一种工具，可维护不同群体的权利和利益：普通公众、负责保护公众利益的机构，以及商业选区和知识产权选区。GAC 认为，目前拟议的这种做法可能会影响 SSAD 的稳定性和可预测性。

---

68 第 8 项、第 5.3 项和第 5.4 项建议。***另请参阅*** 2020 年 5 月 22 日 ICANN 首席执行官致欧洲数据保护理事会的信函，https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf。

69 *请参阅* 2020 年 5 月 22 日 ICANN 首席执行官致欧洲数据保护理事会的信函，https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf（“关于如何在访问数据的合法利益与数据主体的利益之间取得平衡的不确定性，很大程度上取决于注册服务机构的主观判断和自主决定。作为接收访问请求的控制方，注册服务机构可酌情决定是授予或是拒绝访问非公开 gTLD 注册数据的请求。”）。

70 另请参阅《注册目录服务第 2 审核小组最终报告》（2019 年 9 月 3 日）中的第 5.2.1 节，以及反网络钓鱼工作组与信息传递、恶意软件和移动反滥用工作组的联合调查报告（2018 年 10 月 18 日）。

71 第 5.3-5.5 项建议。此外，实施指南甚至不要求签约方调整其对于披露决定的分析，“以遵守解释 GDPR 的适用案例法、EDPB 发布的指南，或者对 GDPR 或未来可能出现的其他适用隐私法的修订”。*请参阅*第 8.17 项建议。该实施指南使用的是“应该”而不是“必须”一词，因此不具备强制执行性（请参阅 ICANN 代表在 2019 年 12 月 19 日致 EPDP 团队的电子邮件，其中对“应该”和“必须”这两个词的强制执行性进行了讨论。）

优先处理那些会引起消费者保护问题的请求

GAC 担心无法充分优先处理消费者保护请求（会引发与网络钓鱼、恶意软件和欺诈相关的问题），从而导致引起通常需要立即采取相应措施的[72]广泛公众关注和担忧。[73]现有的建议将消费者保护请求置于三个优先级别中的最低级别。此外，管理第 3 优先级请求响应时间的相应服务级别要求规定的响应时间太长：在实施的前六个月，需在五天之内响应；此后，响应时间加倍，延长至 10 天。[74]缺乏优先级顺序和较长的响应时间，可能会导致欺诈以及网络攻击迅速造成重大危害。GAC 建议，将消费者保护请求指定为第 2 优先级。

即使人们接受了当前指定的第 3 优先级，但拟议的第 6 项建议中提出的执行方案也引起了人们的担心。GAC 接受以下事实：该建议要求请求者能够标记会引起消费者保护问题的请求（“请求者‘必须’能够表明披露请求涉及消费者保护问题。”）。[75]但是，该建议并不包含类似的强制性要求，即，要求签约方将消费者保护相关请求置于同等优先级别的其他请求之上并优先处理。这些建议没有使用“必须”一词，而是指出签约方“应该”优先处理这些请求。[76]然而，ICANN 合规部曾明确告知 EPDP 团队，使用“应该”一词不会产生强制性义务。[77]因此，该建议在本质上是相互矛盾的，因为它要求能够识别消费者保护问题，但却未要求签约方针对此项指示采取相应措施。EPDP 团队关于这个问题的讨论得出的结论是，只需使用排序机制即可实现这个目标。但是，由于与消费者保护相关的请求会引发影响 DNS 整体安全性的问题，因此 GAC 建议强制性要求（不是允许）优先处理此类请求。

可靠的 SSAD 改进机制

与任何新系统一样，SSAD 在实施和应用方面也面临挑战，并且需要及时做出回应。具体包括：可能需要调整机制，来自数据请求者的需求可能会起伏不定，可能会出现数据的新用途和意外用途，尤其是在网络安全领域。因此，有必要逐步改进 SSAD，调整机制以解决新障碍，并对新的法规作出响应。

至于自动化主题，“关于自动化披露决策的最终建议”要求对所有类别的请求进行自动化处理，因为自动化被确定为“在技术层面和商业层面是可行的，并且在

---

72 GAC 还指出，消费者保护请求的拟议定义似乎限制性过强，并且要求将拟议的括号中内容解释为是说明性文本，而不是综合性文本。

73 *请参阅* SSAC 关于 gTLD 注册数据临时规范第 2 阶段快速政策制定流程初步报告的意见 *(*SAC 111)，第 9-10 页。

74 第 6.2 项、第 10.4 项和第 10.11 项建议。

75 第 6.2 项建议。

76 第 6.2 项建议

77 *请参阅上文脚注 14*

法律层面是允许的。”[78]尽管 EPDP 团队审议了一系列自动化用例，但却只能同意将两个用例纳入最终报告。[79]包括 GAC 在内的一些利益相关方团体曾设想 SSAD 会提高自动化和集中化处理水平，因为正如比利时数据保护机构的代表们认为的那样，集中式模型在安全性和数据主体方面“似乎是更好的‘常识性’选项”。[80]尽管如此，GAC 和部分其他利益相关方团体仍同意采用这种“混合”模型而不是集中式模型，条件就是最终建议应提供一种赋予 SSAD 灵活地演变和发展的机制，且无需因每次调整而开展新的政策制定流程以便与最终报告保持一致。

第 18 项建议提出设立一个由参与 EPDP 的所有利益相关方团体代表组成的常任委员会，负责处理这些决定。但是，GAC 认为，尽管第 18 项建议规定了对政策建议实施情况进行审核，但是似乎没有达到提供一套实现 SSAD 高效演进机制的目标。特别是，关于以下内容没有清晰的说明：自动化的新用例是否包含新政策或现有政策实施。GAC 还指出，如果每个新用例都被视为是需要新 PDP 的新政策，那么现阶段尚不清楚 SSAD 是否会有效演变，尤其是是否会向更集中化的方向发展。在这种情况下，伴随着对分散处理的各种担心，SSAD 可能依然是一个分散式的系统。因此，GAC 要求 GNSO 理事会确保 EPDP 建议在这方面提供足够的确定性，以便当满足“在技术层面和商业层面是可行的，并且在法律层面是允许的”测试条件时，允许进一步提高自动化。

提出变更的其他要求甚至包括：不仅要获得常任委员会的一致同意，而且要获得签约方的批准。然后，这些建议需要得到 GNSO 理事会（缺少来自咨询委员会的代表）的批准才能通过。这个“演进”过程可能会变得复杂而漫长，且不适用于处理需要迅速采取果断措施的实施问题。

财务可持续性

根据这些建议，可能会建立一个对其目标用户（包括调查和打击网络安全威胁的 SSAD 用户）来说过于昂贵的系统。建议指出“数据主体‘不得’承担向第三方披露数据的费用；SSAD 数据的请求者应主要承担维护此套系统的费用”。[81]尽管 GAC 注意到了当其他人希望访问注册数据时不向注册人收取费用的这种呼吁，但同时 GAC 也指出，注册人在注册域名时要承担全部域名注册服务的费用。正如 SSAC 最近指出的那样：

> 此类费用应包括：向有权获取修订数据的第三方披露信息，以完成合法的安全、稳定与弹性 (SSR) 活动，以及可能不属于

78 第 9.3 项建议。

79 *请参阅*第 9.41 项和第 9.42 项建议（第 9.43 项和第 9.44 项建议与只针对城市字段或不包含个人数据的记录的狭窄请求类别有关）。

80 https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority

81 第 14.2 项建议。

> SSAC 活动范围的其他法律活动（例如，权利保护）。确保 DNS 的总体安全、稳定与弹性要求能够访问此类注册数据，以便与受损资源的所有者进行通信交流，以及确定欺诈和恶意活动，从而中止犯罪分子获得的注册服务。[82]

此外，GAC 还指出，SSAD 的大部分费用与其普遍使用人工手动（相对于自动化）处理有关，这种方法本质上存在可扩展性限制和固有的高成本缺陷。SSAD 的财务可持续性与它对人工处理的依赖密不可分。尽可能减少人工手动处理将有助于提高 SSAD 的财务可持续性。[83]总的来说，与为开发 SSAD 提供资金支持有关的建议可能难以实施，并且可能会引发更多无法解答的问题，特别是：1) ICANN 会在多大程度上为开发该系统提供资金支持；2) 注册服务机构会在多大程度上将 SSAD 的成本转嫁给客户；3) 请求者在设置和批准系统使用费用等方面扮演着什么样的角色等等。GAC 认为，可取的做法是“正式评估系统对用户的影响以及对安全性和稳定性的影响”。[84]

EPDP 第 2 阶段最终报告中未解决的问题

数据准确性

《EPDP 章程》要求 EPDP 团队负责评估“披露框架 [……]，以解决 (i) 涉及滥用域名注册数据的问题，包括但不仅限于消费者保护、网络犯罪调查、DNS 滥用以及知识产权保护，[和] (ii) 解决适当的执法需求”。用于这些目的（实际上对于任何目的，包括签约方联系其客户的能力）的域名注册数据是否有效取决于数据的准确性。而且，注册数据的准确性是 GDPR 的一项基本要求，EPDP 第 1 阶段最终报告曾指出，“*预计将进一步审议与 GDPR 合规要求相关的数据准确性问题*”。因此，最终报告中没有关于这一重要主题的任何建议，GAC 对此表示关切。

正如 GAC 之前强调的那样：

> 域名注册数据的准确性是确保 GDPR 合规，以及实现维护一个安全且富有弹性的 DNS 这一目标的基础。GDPR 和其他数据保护制度以及 ICANN 的《注册服务机构认证协议》均要求数据准确，这种准确性对于 ICANN 履行自身肩负的“确保 DNS 的安全性、稳定性、可靠性和弹性”职责至关重要。正如欧盟委员会在 2018 年 2 月 7 日致 ICANN 的信函中所述：“*根据欧盟数据保护法律框架的规定，以及签约方在其与 ICANN 签订的合同中规定的义务，应确保个人数据准确并及时更新。考虑到数据处理*

[82] SAC 111。

[83] 鼓励减少人工手动处理的另一个主题是：探索签约方可以实施哪些法律允许的机制，以允许数据主体在域名注册时自由地同意或反对披露其数据。这将推动对受保护信息数据库和不受保护信息数据库的维护，进而开启将不受保护的信息数据库转向低成本的自动化处理之旅。

[84] *请参阅* SAC 111。

> *目的，必须采取一切合理措施，确保立即删除或更正不准确的个人数据 [……]。为满足数据质量要求，应采取合理举措确保获得的个人数据准确无误。”*[85]

为遵守 GDPR 的规定，确保“与处理数据的目的”相关的数据准确性和数据质量至关重要。[86]披露的数据不准确不仅违背了 SSAD 的宗旨，而且存在违反数据保护法规的风险。准确性是全球大多数数据保护法中一项核心的数据保护原则。特别是 GDPR 第 5 条中规定了数据准确性要求。

为提高 WHOIS 数据准确性而制定的现有合同要求的准确性似乎不甚明朗。近期的审核小组报告对验证程序的有效性提出了质疑，例如 RDS 审核小组报告和 CCT 审核小组报告，这两份报告都得到 GAC 的支持。[87]此外，自 2014 年以来，WHOIS 数据准确性投诉在向 ICANN 合规部报告的关于注册服务机构的投诉中占据最大比例，是单项投诉最多的一类。[88]

因此，GAC 呼吁 GNSO 理事会要求当前的 EPDP 团队解决这一问题，以便将数据准确性作为 SSAD 一个不可或缺的组成部分。

自然人/法人

在 2020 年 6 月 27 日的 ICANN 第 68 届会议 GAC 公报中，GAC 要求 GNSO 尽快提供其在制定具体规划以继续完成政策制定流程这方面工作的最新进展情况，以解决与区分自然人和法人实体相关的未决问题。这个问题很重要，因为包括 GDPR 在内的个人数据保护条例仅适用于自然人，且只保护自然人的个人数据处理。[89]根据包括 GDPR 在内的个人数据保护条例，如果不允许识别个人身份，则关于法人的信息不被视为个人数据。因此，签约方可以公开此类法人数据，而不会引发数据保护担忧。然而，正如最终报告中所述，注册服务机构和注册管理运行机构将

---

85 GAC 关于第 2 阶段附录的意见。

86 *请参阅* GDPR 第 5(1)(d) 条。*另请参阅*英国信息委员会办公室关于 GDPR 的指南（适用于组织机构的指南），https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

87 *例如，请参阅*注册目录服务 WHOIS 2 审核最终报告第 49-61 页（其中指出，WHOIS 数据不准确率依然较高并且可能低估和少报）；政府咨询委员会关于 RDS-WHOIS2 审核小组最终报告的意见（2019 年 12 月 23 日）第 5-7 页；以及 竞争、消费者信任和消费者选择审核小组最终报告第 103-106 页。*另请参阅*WHOIS 审核小组报告（2012 年 5 月 11 日）第 11-13 页（“低准确率的 WHOIS 数据是不可接受的，这会降低消费者对 WHOIS 系统和整个行业的信任，由于 ICANN 在这个行业中负责制定规则并发挥协调作用，因此，也会降低消费者对 ICANN 自身的信任”）。

88 *请参阅*《ICANN 合同合规部年度报告》中关于注册服务机构的详细报告内容（2014-2019 年），https://features.icann.org/compliance/dashboard/report-list。

89 GDPR 不包含涉及法人的个人数据处理规定，特别是作为法人成立的企业，例如法人的名称和形式，以及法人的详细联系信息（GDPR 第 (14) 条）。“虽然法人的详细联系信息不在 GDPR 的约束范围内，但是自然人的详细联系信息，以及与已识别或可识别的自然人相关的任何其他信息都在 GDPR 的约束范围内”（*请参阅 2018 年 7 月 5 日* EDPB 致 ICANN 的信函）。

继续*被允许*但是*没有义务*区分法人和自然人注册数据。[90]这种做法不能“最大限度地确保 WHOIS 数据的持续可用性”[91]，并且最终报告没有提供用于进行这种区分的推荐程序，违背了第 1 阶段 EPDP 团队和 EPDP 团队章程的明确指示。[92]

屏蔽法律允许公众继续访问的数据这种做法会产生巨大影响，因为大量域名是由法人实体注册的。2013 年 ICANN 委托进行的一项研究表明，**法人实体在域名注册人中所占比例最高**。[93]公众评估某个网站的合法性以及执法机构找出网站背后的实体的一种方法，就是查阅公开的域名注册信息，其中应包含法人实体的数据。

值得注意的是，EPDP 团队收到的法律指导建议采取几个步骤来降低责任风险。[94]此类指南的含意是，可以采取多种措施来确保注册人准确地将自己指定为法人实体。需要注意的是，某些国家和地区顶级域（包括欧盟范围内的国家和地区顶级域）已经公开提供了法人实体注册人的某些数据，这表明区分自然人和法人的做法在法律层面上是允许的，也是可行的。[95]

此外，区别对待法人和自然人数据还与自动化处理这个问题密切相关。如上所述，法人数据不受 GDPR 保护。因此，在注册过程中区分法人和自然人可能包括将法人数据分配到应自动处理其数据的人员类别中。[96]

GAC 认为，解决法人和自然人的区分问题，不仅是使整个 SSAD 模型达到其目的关键，同时也是符合适用数据保护法的做法。因此，GAC 要求 GNSO 理事会竭尽全力解决此问题。在这方面，GAC 重申了自己的诉求，要求 EPDP 团队重点关注已收到的法律指导意见，以制定合理的政策来允许法人实体信息保持公开。

---

90 *请参阅* EPDP 第 2 阶段最终报告第 2.3 节“第 1 优先级和第 2 优先级主题”。

91 *请参阅 ICANN 数据保护/隐私问题*网页：https://www.icann.org/dataprotectionprivacy

92 *请参阅 EPDP 团队章程*：https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf （包括指示团队审议是否应该允许或要求签约方区别对待法人和自然人，以及需要采用哪些机制来确保做出可靠的状态决策）。

93 *请参阅 WHOIS 注册人识别研究*：https://gnso.icann.org/sites/default/files/filefield_39861/registrant-identification-summary-23may13-en.pdf 基于我们对从排名前五位的 gTLD 中随机抽取的 1600 个域名中检索到的 WHOIS 记录展开的分析，

- 39% (± 2.4%) 的域名似乎由法人注册
- 33% (± 2.3%) 的域名似乎由自然人注册
- 20% (± 2.0%) 的域名通过隐私或代理服务注册。
- 我们无法使用 WHOIS 中的可用数据对剩余的 8% (± 1.4%) 的域名注册人进行分类。

94 *请参阅 Bird & Bird* 关于《通用数据保护条例》(GDPR)（条例（欧盟）2016/679）要求注册人自我识别为自然人或非自然人的责任的建议（建议的方法包括：撰写清晰明了的通知语言，避免使注册人产生任何误解或错误；确保注册人了解注册为法人实体的后果，以及验证联系人信息不包含个人数据）。

95 *例如，请参阅*比利时 (.BE)、欧盟 (.EU)、爱沙尼亚 (.EE)、芬兰 (.FI)、法国 (.FR)、挪威 (.NO) 等。

96 作为一项保护措施，享有增强型法律保护的人员可能会被分配到非自动查询组。这类人员可能包括：受国家法律（例如，银行保密法）保护的法人、受特定法律保护（例如，法院保护令）的自然人、处于弱势地位的数据主体（例如，儿童、寻求庇护者、其他受法律保护的阶层），以及默认情况下，提供肯定的个人隐私权保护的司法管辖区内的所有国民。

匿名电子邮件地址

使用匿名电子邮件可能是一种一举两得的解决方案：一方面保护注册人身份，同时为部分出于合法目的请求访问域名注册数据的人提供服务。最终报告在第 2 优先级事项中列出了“唯一联系人拥有统一的匿名电子邮件地址的可行性。”[97]EPDP 团队收到的法律指导意见是，匿名化和假名化是“一项有用的隐私增强技术/隐私设计方案”。[98]正如该法律指导意见所认可的一样，GAC 想要指出的是，匿名化处理后的信息不在 GDPR 的约束范围内。[99]虽然 GAC 承认匿名信息与个人数据之间可能存在关联，但是 GAC 赞同该法律指导意见的观点，即，匿名化是一种有用的隐私增强技术，因此应对其展开进一步的研究。

鉴于上述情况，GAC 认为需要展开进一步的可行性分析，以更好地了解这个方案的优势和风险，而不是在没有进一步调查的情况下就不予考虑。

控制权

最终报告中提到，签约方与 ICANN 组织之间或许可以拥有联合控制权。然而，GAC 希望能够更加清晰地阐述 SSAD 模型中每个数据控制人和数据处理人的地位和作用。具体而言，GAC 希望制定具体的数据处理协议，更清楚地说明在采用不同方式处理数据时，如何分配签约方与 ICANN 组织各自所承担的责任。GAC 呼吁 GNSO 理事会应要求 EPDP 团队进一步解决这一问题。

结论

GAC 赞赏参与 EPDP 第 2 阶段工作的所有利益相关方、支持人员以及 EPDP 主席所付出的辛勤努力，感谢他们持续积极参与这些重要的公共政策事务。最终报告中有许多值得称赞的内容。但是，GAC 也认为，某些关键建议和未解决的主题尚需进一步跟进，因此，GNSO 理事会应要求 EPDP 团队根据这份少数派声明中提出的要点完成相关工作。GAC 期待与我们的同事们在这些重要问题上继续开展交流合作。

97 EPDP 第 2 阶段最终报告，第 3 页。

98 Bird & Bird 关于标准化访问/披露系统 (SSAD)、隐私/代理和假名化电子邮件的“第二批次”GDPR 问题的法律指导意见（2020 年 2 月 4 日）。

99 *请参阅* GDPR 第 26 条。

非商业利益相关方团体 (NCSG) 的少数派声明

NCSG 不同意第 22 项、第 20 项和第 7 项建议，原因如下

第 22 项建议：目的 2

第 22 项建议中的“目的 2”目前内容如下：*“根据 ICANN 使命，促进维护域名系统的安全、稳定与弹性。”*

NCSG 强烈反对这一目的。措辞过于模糊和宽泛，允许 ICANN 采用其认为合适的任何方式处理 gTLD 注册数据。贝基 • 伯尔在一封代表 ICANN 董事会发送给 EPDP 团队的电子邮件中承认，它对 ICANN 组织的所有要求，就是找出与《ICANN 章程》解释相符的理由。

在那封邮件中，伯尔指出：*“根据《ICANN 章程》的规定，维护域名系统的安全、稳定与弹性 (SSR) *是* ICANN 的使命。《ICANN 章程》第 1 条第 1.1 节明确规定：ICANN 的使命是确保互联网唯一标识符系统的安全稳定运营。章程本身还从域名、根服务器系统、数字和协议的层面出发，提供了诸多关于该项使命的职责范围的详细说明。”*

在第 1 阶段，我们制定了针对每项 ICANN 目的的工作表，其中详细说明了所有这些目的的法律依据和流程活动。但第 2 阶段没有做到这一点。因此，重新制定的目的 2 没有说明为什么需要披露数据，也没有说明向谁披露数据，更没有说明为什么需要保留数据以及这些数据要保留多长时间。此外，目前第 2 阶段最终报告中草拟的目的 2 也与 GDPR 的目的限制原则——第 5(1)(b) 条相冲突，后者要求*“出于特定、明确和合法的目的收集数据，且不得以与这些目的不相符的方式进一步处理数据”*。确保互联网唯一标识符系统的安全稳定运营 (SSR) 既不具体，也不明确，而 ICANN 董事会对 ICANN 职权范围内的安全运营的解释更是不清不楚。

NCSG 已在多个场合要求 EPDP 团队就以下问题达成共识：ICANN 在 SSR 方面所肩负的使命，以及 ICANN 在处理 gTLD 注册数据请求时如何践行这样的使命。尽管为此需要履行 ICANN 作为数据控制人的法律义务，但这些请求一直遭到 ICANN 的拒绝。

EPDP 团队尚未成功地就 ICANN 使命中的 SSR 如何适用于此目的达成共识，ICANN 也未表明自己对此有何洞见。然而，与 GDPR 中的其他法律依据一样，第 6(1)(f) 条也规定了数据控制人对数据主体的其他义务，包括保护数据主体的权利和利益。

英国信息专员办公室在其关于使用第 6(1)(f) 条作为法律依据的指导意见中指出，当以人们预期的合理方式使用数据且对数据隐私造成的影响最小时，使用这一条

款作为法律依据最合适。gTLD 注册人对 ICANN 为什么或如何基于目的 2 来披露或保留数据几乎没有任何预期。ICANN 或 EPDP 团队并没有发现这些未知情况，注册人对这些情况有所了解的唯一途径是，注册 gTLD 域名是否要求注册人也具备解释和应用《ICANN 章程》的专业知识。这样的预期并不现实；这超出了 ICANN 内部工作人员、董事会成员以及 EPDP 团队成员的能力范围。

NCSG 认为，目的 2 实际上不是 ICANN 履行其使命所必需的，将其纳入最终报告是为了 ICANN 组织能够满足第三方的愿望，尽管在修订后的建议中删除了对第三方合法权益的提及。尽管这种做法完全无视了 GDPR 赋予数据主体的权益，但是 ICANN 董事会似乎认为，这项法律基础为其提供了责任保障。

为了对注册人公平，需要将目的 2 细分为多个明确阐述的目的，以便明确规定要展开哪些流程活动，并简洁明了地向注册人传达和解释。

第 20 项建议：城市字段

NCSG 认为，将 EPDP 第 1 阶段关于“城市字段”的建议从“必须”修订改为“可以”修订，并没有令人信服的理由。要求修订此字段的先前建议是基于 Bird & Bird 提出的法律建议，其中指出：

> *“3.16 考虑到上述所有情况，相关方也许能够满足公布“城市”字段的合法权益测试的要求。然而，从目前获得的信息来看，我们对此并不清楚。尤其是：*
>
> *a) 需要提供进一步的信息，以表明赋予权利持有人的利益具有足够的意义，从而有理由普遍公布城市字段，而不是在非常有限的情况下才能使用城市字段；以及*
>
> *b) 需要提供更多有关对数据主体权益的潜在影响的信息。*
>
> *3.17 然后，相关方需要对事实和具体情况进行详细评估，以确定所追求的利益是否凌驾于数据主体的利益之上。”*

这清楚地表明，需要进行平衡测试，以权衡寻要披露 gTLD 注册数据的第三方的合法利益与相关注册人的权利。NCSG 深信，作为处理披露请求的一部分，这需要通过 SSAD 来进行，并且不应与 ICANN 处理 gTLD 注册数据的目的混为一谈，后者正是 EPDP 第 1 阶段建议所涵盖的内容。

Bird & Bird 在致库尔特 • 普里茨 (Kurt Pritz) 的电子邮件中重申了这一发现，他们指出，*“法律分析很清楚，这是个人数据；原则上，可以根据权利持有人的合法利益证明公布相关数据是合法的，除非个人利益凌驾于合法利益之上。*

这如何适用于以下客观事实：确认权利持有人是否拥有足够的利益，如何平衡权利持有人与注册域名持有人的利益，这些问题都不明确。”

所有这些都高度暗示了，应该像对待所有其他个人信息一样，必须修订 gTLD 注册数据中的“城市字段”。

第 7 项建议：请求者目的

NCSG 坚持不同意列入一个脚注，用于说明欧盟 NIS 指令是一项对受监管实体规定其义务的立法典范。这个示例是 EPDP 团队在微调最终报告和建议期间添加到建议内容中的，目的是为了获得尽可能多的支持，而 NCSG 则认为，EPDP 团队没有给予足够的时间或关注就将这一示例纳入最终报告，也没有充分考虑会对允许向第三方披露的政策带来的影响。

此外，NCSG 还认为，排除这个示例不会对 NIS 指令或其他类似条例规定的适用实体要求 SSAD 披露经修订的 gTLD 注册数据的能力产生任何有意义的影响。

注册服务机构利益相关方团体 (RrSG) 的少数派声明

EPDP 第 2 阶段最终报告代表着 ICANN 社群多年合作的凝聚成果。RrSG 一直认为，制定政策和开发系统以实现注册服务机构的数据保护要求与出于合法目的而依赖访问非公开注册数据的人员的需求之间的平衡，这符合我们各方的利益。

在整个 EPDP 第 2 阶段中，注册服务机构都非常关注开发、部署和运营 SSAD 的合法性、技术可行性和相关成本等问题。虽然注册服务机构比其他相关方更支持某些建议，但这些建议都是高度相互依赖的，必须整体考虑，而且我们认为整体考虑的最终结果大于各部分的总和。

因此，本着与其他利益相关方不断采取折中方案的精神，我们支持 EPDP 第 2 阶段的成果和这份最终报告中的建议，我们将遵守由此产生的共识性政策。

我们认为，最终建议应该为建立一个标准化和可预测的系统提供足够的指导，既充分考虑 EPDP 第 1 阶段的建议，同时也给予每个注册服务机构足够的灵活性，使他们能够根据通常涉及多个司法管辖区的法律和隐私相关义务采用适当的方式实施其 SSAD 业务。

我们敦促 GNSO 理事会和 ICANN 董事会采纳报告中的所有建议，以便我们能够过渡到执行工作并迅速启动 SSAD。

注册管理机构利益相关方团体关于 EPDP 第 2 阶段最终报告的声明

注册管理机构利益相关方团体 (RySG) 赞赏 EPDP 团队在第 2 阶段所做的工作，认可 SSAD 对第三方的效用，并且支持最终报告中包含的建议。这些建议反映了 EPDP 团队在尽最大努力制定个人数据访问解决方案，以在保护数据主体的隐私权与第三方的合法权益之间取得平衡。虽然这一声明提及了对最终报告某些方面内容的关切，但是我们接受构成 SSAD 建议基础的折中解决方案。我们对 SSAD 的未来发展依然保持乐观。

在一年多的尽职调查中，注册管理机构始终坚持以下原则，即：此系统必须 (i) 反映当前数据保护法的现实情况，(ii) 优先考虑并适当保护注册人的个人数据，而不是第三方的利益，以及 (iii) 保持我们作为控制人的能力，以履行我们保护个人数据的法律义务。有些人对基于这些原则的系统表达了不满。尽管如此，我们仍然认为这些原则是保护注册人个人数据和履行法律义务的最佳方式。

RySG 的真诚参与

EPDP 团队经许可负责“确定 gTLD 注册数据临时规范在保持原样或略作修改的情况下，是否应该成为一项 ICANN 共识性政策，同时确保该规范符合 GDPR 和其他隐私性和数据保护相关法律的规定。”[100]章程规定，只有当主要问题“在准备临时规范初步报告过程中得到解答并最终确定”之后，才能开始评估系统开发事宜，以利于第三方访问注册人个人数据的辅助工作。[101]第 1 阶段最终报告已于 2019 年 2 月 19 日发布，其中包含一项详细且可强制执行的建议，旨在实现第三方获取注册人个人数据的流程的标准化。[102]

RySG 积极参与了第 2 阶段开发系统的工作，以便拥有合法权益的第三方可以访问注册人的个人数据。注册管理机构不需要这样的系统来履行我们保护注册人个人数据的义务，以及响应第三方获取此类个人数据的请求。根据第 1 阶段报告的要求和我们的法律义务，目前在没有 SSAD 系统的情况下，我们的成员也在定期负责任地响应各种数据请求。即使 SSAD 投入运营，我们仍将继续这样做。遗憾的是，SSAD 可能会给注册人个人数据带来额外的处理流程和风险，从而使我们的工作任务在许多方面更难展开。

我们以开放的心态听取了那些坚持想要更多地访问个人数据的社群的意见，并且积极参与了这一进程，以便找到适当的解决方案。虽然我们支持最终报告和团队提出的折中方案，但出于下列原因，我们对社群在实施这些建议过程中仍需持续努力表示高度关切。

[100]EPDP 团队最终采纳的章程 – 2018 年 7 月 19 日，位于此处。
[101]EPDP 团队最终采纳的章程 – 2018 年 7 月 19 日，位于此处。
[102] *请参阅* EPDP 第 1 阶段最终报告第 18 项建议，位于此处。

RySG 优先考虑数据保护

在这些讨论中，我们的出发点始终是数据保护原则。常规的数据保护法规，尤其是 GDPR，主要“保护自然人的基本权利和自由，特别是自然人保护他们个人数据的权利”。[103]正如欧盟委员会最近重申的那样，“GDPR 的最终目标是改变所有参与各方的文化和行为，*以保护个人利益*”。[104]简单来说，数据保护的重点就是保护个人的个人数据。尽管这一原则应该是不会引起争议的，但我们过去两年的经验表明实际情况并非如此。[105]

在实践中，确定数据保护的优先级是指在考虑如何处理数据以及由谁处理数据所带来的影响时，应将数据主体放在首位。这意味着，默认情况下将数据最小化和数据隐私作为基准，以避免对任何个人的个人数据进行不必要的处理。这意味着，确保我们不实施那些限制我们作为数据控制人履行自身法律义务的能力的政策要求，以充分保护个人委托给我们的个人数据。

尽管存在这些原则，我们在工作中仍然不断展现灵活性，并努力关照第三方的利益，即使这样做要求我们做出让步，也可能会增加签约方的风险。虽然有些相关方希望我们做出进一步的让步，但是当第 2 阶段独立法律顾问、数据保护机构，以及掌握欧盟数据保护法规专业知识的 CPH 成员反复告知并要求我们在一些方面做出让步时，我们必须划定自己的底线：某些要求是不合法的，或者会对数据主体构成重大风险。

第 2 阶段的工作目标是实现第三方请求访问注册人个人数据的流程的标准化。然而，经过几个月的分析，持续坚持寻找一种途径以实现事实上的自动化访问个人数据，这种做法不利于数据主体。我们非常担心，不惜任何代价追求自动化访问的做法将最终损害 SSAD 的合法性及其未来的可用性。

混合模型反映了法律要求与实践现实

混合模型（即，集中接收和分散决策）是一种实用的解决方案，我们认为它会解决请求者提及的关于请求访问注册人个人数据的方法现状的许多问题。最重要的是，混合模型反映了在当今法律规定下可能发生的现实。

Bird & Bird 确认责任应归于数据控制人，甚至设想开发一个完全集中式的自动化系统以取消签约方的酌情处理权，“最可能的结果，当然也是大多数监管机构的出

[103]GDPR 第 1 (2) 条。

[104]欧盟委员会致欧洲议会和欧洲理事会的信函，2020 年 6 月 24 日，第 5 页（着重部分由作者标明），位于此处。

[105]虽然《基本权利宪章》第 17 条承认“知识产权应受到保护”，但欧洲议会已经澄清，行使该项权利“不得妨碍保护个人数据，包括互联网上的个人数据。”请参阅欧洲议会和欧洲理事会 2004 年 4 月 29 日关于知识产权执法的第 2004/48/EC 号指令，位于此处。

发点，就是‘签约方即数据控制人’”。[106]而且，比利时数据保护机构强调，控制权是一个事实性的角色，相关方“不能随意简单地‘指定’”，并且“根据共同协定也不能放弃”。[107]

我们接受 Bird & Bird 以及 DPA 关于这个问题的建议，并且早在一月份，我们就曾谨慎地提出，“对完全集中式模型的进一步审议，只会分散我们的注意力，以及延迟我们及时且成本高效地完成工作任务。”[108]遗憾的是，即使是在 EPDP 的后期阶段，我们依然还会不断听到关于以下问题的建议，例如：如何对注册人的个人数据进行集中决策，以及如何通过我们的政策建议来分配控制权。[109]

自 EPDP 同意拒绝采用集中式模型以来，一切都没有改变，因为集中式模型不符合减轻签约方责任的前提条件。[110]我们担心的是，一些相关方要么不理解，要么故意忽略与其首选政策结果不一致的法律建议。这两种情况都不适合就可执行的政策建议达成共识。

即便是“集中式模型”这个术语，也没有准确反映出提倡采用这种模型的人实际上的主张具体是什么。只有决策，而不是实际数据本身，一直是“集中式”系统讨论的一部分。如果没有底层数据处理，这就不是“集中式”系统，它将会限制不必要的数据处理并增强数据主体的安全性。相反，这种系统不仅会增加额外的不必要的处理步骤，而且默认情况下不符合数据最小化和数据隐私的基本原则。

尽管导致我们最初拒绝采用集中式模型的客观事实没有发生任何变化，但是我们依然非常关切这个问题：部分群体坚持认为“集中化”的个人数据披露方式在 ICANN 生态系统中是合法且切实可行的。虽然我们支持 ICANN 努力寻找在集中式系统下如何分配各方责任的答案，但是仍然没有指导意见表明转移先决条件责任在法律层面是可能的。

[106]菲尔 • 布拉德利 • 施米格 (Phil Bradley-Schmieg) 和露丝 • 博德曼 (Ruth Boardman) (Bird & Bird LLP)“问题 1 和 2：责任、保障措施、控制人和处理人”，2019 年 9 月 9 日，第 6 页，2.18。

[107]数据保护机构（比利时），致马跃然 (Goran Marby) 的信函，2019 年 12 月 4 日，第 3 页，位于此处。

[108]CPH 后续步骤信函，2020 年 1 月 7 日。

[109]例如，请参阅 2020 年 7 月关于建议 9 的第 2 类意见，尽管收到了相关法律建议并且一致同意采用混合模型，但 IPC/BC 提出了“通过 CGM 的集中决策实现非自动化的概念”：“根据收到的法律指导意见，EPDP 团队建议，按照 GDPR 的规定，当采用手动处理且从头开始审核时，在法律层面上允许中央网关经理对以下类型的披露请求进行集中化披露评估（披露决定的接收和处理）：

- 针对明确的‘域名匹配商标’请求的自动化披露决定
- 针对明确的网络钓鱼案例的自动化披露决定
- ICANN 组织是处理这一披露决定的控制人。”

[110]“因此，这意味着，从本质上来说，要部署任何统一访问模型，要么得与 2500 个签约方就他们认为的法律风险达成一致，要么提出一项动议（原文如此），减轻签约方的法律责任。”马跃然，EPDP 团队面对面会议文稿，2018 年 9 月 25 日，第 2 页，位于此处。

GNSO 常任委员会

RySG 支持“SSAD 应该是灵活的，并且能够根据变化的法律或实际情况进行调整”这样一个概念。我们认识到，SSAD 必须灵活，并且能够适应不断变化的行政指导、法院判决以及各个司法管辖区的新条例。但是，我们反对 GNSO 常任委员会的工作必须取得预定成果的观念。也就是说，我们不能接受这样一种假设：即 SSAD 在未来将会不可避免地朝着更加集中化和更加自动化的个人数据披露方向发展。SSAD 的演变必须基于事实和数据，而不是假设和猜测。

如上文所述，混合模型反映了在当今法律规定下可能发生的现实。如果混合模型有一天会演变为集中式模型，那我们不同意采用混合模型，因为我们无从知晓法律未来会有什么变化。我们同意混合模型是改善现状，同时仍可充分保护个人数据的一种解决方案。

在其各自所属的利益相关方团体中，EPDP 工作组的成员应该对 SSAD 随着时间的推移可能产生的演变这个问题设定适当的预期。尽管这个系统可能会朝着某些 EPDP 成员预期的方向发展，但同样（如果不是更大可能性的话），这个系统也可能会变得更具限制性、自动化程度更低，或者更加分散。[111]在社群的某些成员看来，将系统演变描绘成一条单行道而不是对事实和数据的合理响应，这种做法会使系统陷入失败。

同样地，虽然我们总体上支持 GNSO 常任委员会的工作范围，但是对于以放弃我们作为控制人的法律义务的方式制定这一机制的做法表示严重关切。我们一直反对明确声明某些变更（例如，添加新的自动化用例）是实施问题还是政策问题的做法，因为我们无法预测针对这些问题未来可能会提出怎样的指导意见。除非欧盟委员会就某个主题提供了完美明确且不容置疑的指导意见，否则基于新指导意见的自动化提案可能会存在遗留的风险、增加额外的义务，或者要求签约方或中央网关经理 (CGM) 修订合同。

我们不难想象到这样的情况：即使是关于额外自动化的简单明确的法律指导，也可能需要进行政策变更。例如，如果发布了新的指导原则，始终允许采用完全自动化，前提条件是在数据处理中发挥任何作用的任何实体都拥有一名 GDPR 定义的指定数据保护主管。目前，我们的建议不要求任何一方（CGM、认证机构、注册管理机构、注册服务机构、请求者）拥有自己的数据保护主管。在这种情况下，如果通过实施将更多自动化用例强加于签约方，而参与数据处理的任何一方未指定数据保护主管，这种做法可能会显著增加签约方的法律风险。

[111]近期就这一方面做出的许多最重要的决定和指导，似乎都表明会进一步加强限制和强制实施，而不是放松要求。*例如，请参阅*案例 C-311/18 数据保护专员诉 Facebook Ireland Limited 和 Maximillian Schrems (Schrems II) 使欧盟-美国隐私保护系统失效；*另请参阅* 2020 年 6 月 24 日欧盟委员会致欧洲议会和欧洲理事会的信函，其中呼吁加强 GDPR 的执法力度而不是放松任何限制，位于此处。

这个例子充分说明了，不预先确定可能涉及法律风险的变更是明确的实施问题而不是政策问题是多么重要的一件事。作为控制人，我们需要能够对我们处理其个人数据的个人所承担的义务做出反应。

只在极少数情况下才有可能实现完全自动化

RySG 支持“在技术层面和商业层面可行，并且在法律层面允许”的自动化概念。[112] 我们认为这些标准是确保数据主体的数据不会受到不合理的自动化处理的必要保障措施。

作为一个出发点，影响数据主体的决策的大规模自动化，由于数据主体从中得不到任何益处，因此通常不符合数据主体的最佳利益，这应该是毫无争议的。如 GDPR 所述，“数据主体应有权不受制于仅基于自动化处理的决定，包括对其产生法律效力或同样对其产生重大影响的特征分析。”[113] Bird & Bird 向我们证实，在收到团队提出的所有可能的自动化用例后，只有四种情况不会对数据主体产生法律或类似的重大影响。[114]

我们从法律意见中得出的结论是，只有一组非常精确定义的决策不会对数据主体产生法律或类似的重大影响。同样，备忘录只评估了遵守 GDPR 要求的那些用例。因此，我们应该谨慎地得出关于法律允许性的宽泛结论，因为相关结论将迫使签约方实施会增加其法律风险的要求。

此外，我们还担心在 SSAD 投入运营的第一天，这四个用例就需要实现完全自动化，[115]尽管 EPDP 团队甚至尚未开始参与关于算法在以下方面的性能的任何技术讨论：(i) 可靠地识别适合进行自动化处理的请求，或 (ii) 以可靠、准确和透明的方式做出决策。我们全体一致认为，自动化必须满足三个条件：(i) 技术层面可行，(ii) 商业层面可行，以及 (iii) 法律层面允许。[116]通过根据法律允许情况要求在 9.4 中添加自动化用例，我们将三个重要的保护措施归结到对这些用例合法性的单个评估中。

事实上，关于算法如何评估建议并做出决定的问题，我们最接近实质性审议的建议是：CGM 应向签约方提供披露建议，同时算法从反馈中了解签约方的披露决定

[112]EPDP 第 2 阶段最终报告，9.3。

[113]GDPR 第 22 条。

[114]EPDP 第 2 阶段最终报告，9.4：(i) 来自当地或其他适用司法管辖区的执法部门提出的要求，其中包括 1) 一项确定的 GDPR 6(1)e 法律依据或 2) 根据 GDPR（第 2 条豁免）进行处理；(ii) 数据保护机构对涉嫌由 ICANN/签约方实施的侵犯数据保护法规的行为进行调查影响到了注册人；(iii) 仅请求访问城市字段，以评估是索赔请求还是出于统计目的；(iv) 签约方先前没有在注册记录中披露任何个人数据。

[115]EPDP 第 2 阶段最终报告，9.4：“根据收到的法律指导意见，EPDP 团队建议以下类型的披露请求，GDPR 已指示法律允许对此类请求进行完全自动化处理（披露决定的接收和处理），从 SSAD 启动时起，必须实现自动化处理。”

[116]EPDP 第 2 阶段最终报告，9.3。

是否与自动化推荐相匹配。[117]这不仅体现了对机器学习一般原理的误解，而且我们对系统提出的建议的可靠性产生了严重的怀疑，因为这个系统并不具备构成我们所做出的决定基础的潜在基础信息。即使我们的决定与充分的规律“相匹配”，这种相关性也不表示算法实际上做出了准确可靠的决定。

需要采用一种更复杂的机器学习和算法训练方法来评估这些用例在技术层面是否可行。这正是要求在审议自动化用例时，将技术层面可行性作为一个重要的独立因素加以评估的原因。如果现在必须致力于确定技术可行性并构建算法工作的相关各方不能成功完成此项工作，那我们就不应陷入强制要求自动化的境地，因为根本不满足技术可行性要求。

财务可持续性需要关注

从第 2 阶段早期开始，RySG 就主张对拟议的 SSAD 进行财务评估，以便为 EPDP 团队的决策提供重要的数据指导。非常感谢 ICANN 团队为我们提供的成本评估。鉴于 ICANN 预估开发和维护拟议的 SSAD 将产生巨额成本，我们担心这一评估在最终报告中被归入一个单独的脚注，特别是在应由 SSAD 用户来承担运营系统的成本这一假设前提下，我们持续收到了其他选区的反对意见。

在此重申我们在审议期间反复提及的一个要点：即，在任何情况下，数据主体均不得向寻求访问其个人数据的第三方提供任何资助。SSAD 旨在提供一个可预测和标准化的系统来访问数据，并且此系统应由直接享受此类服务的人提供资金。

而且，我们支持 ICANN 进行成本效益分析，以确定开发这样一个系统的财务可行性。考虑到第 1 阶段在确立标准化流程以便第三方直接从签约方请求访问数据（第 18 项建议）方面所做的大量工作，双方（数据主体与第三方请求者）都拥有一个用户请求访问个人数据的可预测的流程。而且，任何不希望为 SSAD 服务付费的用户依然可以选择按照第 1 阶段确立的方式提出披露请求，请求者无需支付任何费用。

我们认为，缺乏成本效益分析还指向了一个更大的问题：除了传闻和猜测之外，EPDP 团队从未确定这个系统要解决的实际问题是什么。我们没有看到任何可靠的数据表明签约方对披露要求的回应是一个问题。相关数据实际上表明，大多数正确表述的查询都收到了回复，而未回复的查询通常是：(i) 不适当地请求访问受隐私/代理服务保护的数据，或者 (ii) 在需要提供额外信息时，请求者没有回复。[118] SSAD 无法解决这两类请求者自身犯下的错误。

[117]EPDP 第 2 阶段最终报告，5.1.1，5.5。
[118] *请参阅*在 Tucows 上合法访问隐私和个人数据，2020 年 3 月 13 日，位于此处。

第 2 优先级问题得到解决

虽然 RySG 支持在准确性、法人与自然人，以及唯一联系人的可行性这几个第 2 优先级问题方面展开进一步工作，但是我们反对第 2 阶段没有解决这些问题的说法。事实上，这其中的每一个问题都得到了深入解决，包括对 Bird & Bird 提供的支持维持现状观点的详细分析。我们建议，关于这些主题的进一步工作不应完全从头开始，而应在 EPDP 团队已经针对这些主题所取得的成果的基础上着手。我们认为，在审议这些问题时务必要确保坚持透明和准确原则，以避免社群产生任何误解。例如：

准确性——Bird & Bird 确认，根据 GDPR 的规定，确保数据准确性既是数据主体（而不是第三方）的一项权利，也是数据控制人的义务。[119]而且，Bird & Bird 还确认，《注册服务机构认证协议》中用于确认注册人数据准确性的现有程序，不足以满足 GDPR 对准确性的要求。[120]

法人与自然人——我们不否认 GDPR 适用于自然人数据，而不是法人数据。我们强调指出，实际的挑战是：如何可靠地确定数据到底是属于自然人数据还是法人数据，以及如何处理可能包含自然人数据的法人记录。尽管一些人建议依靠知情同意书作为降低风险的机制，但是 Bird & Bird 确认，依靠知情同意书不是一个容易的解决方案，并且仍然会给签约方带来重大的责任风险。[121]

唯一联系人的可行性——我们收到了关于这个问题的准确的法律指导意见，认为尽管假名化和匿名化是有用的隐私增强措施，但发布掩码电子邮件不符合这些标准条件，因为电子邮件专门用于确保可联系到个人。[122]而且，我们注意到，2020 年 3 月 12 日在全体会议上提交了关于此问题的拟议的建议文本，当时没有收到任何异议，只是不知为何后来却从最终报告中删除了这一内容。[123]

控制人需要具备适当的灵活性来履行其义务

虽然我们支持就第 8 项建议（签约方授权）达成一致所需的折中解决方案，但我们担心该框架已变得过于规范。最初作为披露方‘应该’如何作出决定的指导方

[119]露丝 • 博德曼和凯特琳娜 • 塔西 (Katerina Tassi) (Bird & Bird LLP)，“关于《通用数据保护条例》(GDPR)（条例（欧盟）2016/679）要求的准确性原则的法律建议：对‘法人与自然人’和‘准确性’备忘录查询的跟进”，2020 年 4 月 9 日。

[120]露丝 • 博德曼和加布 • 马道夫 (Gabe Maldoff) (Bird & Bird LLP)，“关于《通用数据保护条例》(GDPR)（条例（欧盟）2016/679）要求的准确性原则的具体含义的法律建议”，2019 年 2 月 8 日。

[121]露丝 • 博德曼 (Bird & Bird LLP)，“关于公开 RDS 中的个人数据并满足《通用数据保护条例》(GDPR)（条例（欧盟）2016/679）要求的知情同意书方案的法律建议”，2020 年 3 月。

[122]露丝 • 博德曼 (Bird & Bird LLP)，“关于标准化访问/披露系统 (SSAD)、隐私/代理和假名化电子邮件的‘第二批次’GDPR 问题的法律建议”，2020 年 2 月 4 日。

[123]“EPDP 团队同意关于以下两个问题的草拟的建议文本，即：唯一联系人拥有统一匿名电子邮件地址的可行性，以及城市字段修订。相关人员支持将这些草拟的建议文本纳入第 2 优先级事项的附录，并发布该附录以征询公众意见。”凯特琳 • 图伯根于 2020 年 3 月 12 日发送给 GNSO EPDP 团队的电子邮件。

针，已变成披露方‘必须’如何作出决定的僵化要求。虽然注册管理机构支持工作组确立的标准化原则，但该政策无法完整考虑具有不同隐私法和法律法规的当地司法管辖区的所有差异，尤其是在跨境提出数据访问请求的情况下。在实施和执行这项建议时必须小心谨慎，以确保披露方有足够的灵活性来说明其特定的司法义务，以避免此建议无法执行。

目的 2

第 22 项建议中关于目的 2 的新文本取代了 EPDP 第 1 阶段第 1 项建议中最初的目的 2，后者未获 ICANN 董事会同意或采纳。我们在此重申第 1 阶段就已提出的关切[124]：此目的不符合 GDPR 所定义的合法“目的”。[125]其中“基于 ICANN 的使命，促进维护域名系统的安全、稳定与弹性”的表述，不知道数据主体是否能够理解他们的数据将如何处理以及必须采用这种方式处理数据的原因。鉴于上述情况和董事会对此目的的支持[126]，以及我们对其预期目的的信心，RySG 同意不反对此目的。

结论

RySG 致力于积极且真诚地参与制定关于注册人数据访问的适当共识性政策建议。我们始终重点关注确保此类建议具备以下特点：提供实现 GDPR 合规的明确途径；商业层面上合理且可实施；考虑到各种不同的商业模型，并且不会阻碍创新。只要满足这些原则以及我们在上文中详述的关切问题，我们愿意就最终报告建议形成共识提供支持。我们期待 GNSO 理事会的进一步审议和批准。

[124]EPDP 第 1 阶段最终报告，RySG 第 1 阶段少数派声明，第 166 页，位于此处。

[125]ICO 关于目的限制的指导意见：“这项要求旨在确保您明确且公开地了解获取个人数据的理由，以及您处理这些数据的方式符合相关个人的合理预期。从一开始就明确自己的目的有助于您对自己的处理方式负责，并避免‘功能潜变’。它还有助于个人了解您会如何使用他们的数据，决定他们是否愿意共享其个人详细信息，并在适当的时候维护其自身对数据的权利。这是建立公众对如何使用个人数据的信任的基础。”位于此处。

[126]马腾 • 波特曼 (Maarten Botterman) 致基思 • 德拉泽克 (Keith Drazek) 的信函，2020 年 3 月 11 日，位于此处。

SSAC：关于《gTLD 注册数据临时规范》快速政策制定流程 (EPDP) 第 2 阶段最终报告的少数派声明——SSAC 112

序言

这是 ICANN 安全与稳定咨询委员会 (SSAC) 关于《gTLD 注册数据临时规范》快速政策制定流程 (EPDP) 第 2 阶段最终报告的少数派声明。

SSAC 主要负责处理互联网名称和地址分配系统安全性与整合性的相关事务。具体包括：运营事务（例如，与正确、可靠运营根区发布系统相关的事务）、管理事务（例如，与地址分配、互联网号码分配相关的事务），以及注册事务（例如，与注册管理机构和注册服务机构的服务相关的事务）。SSAC 致力于针对互联网名称和地址分配服务展开持续的威胁评估和风险分析，以评估稳定性和安全性的主要威胁所在，并据此相应地向 ICANN 社群提出建议。SSAC 不具备监管、强制执行或裁定的职权。这些职能属于其他机构，本报告中提供的建议应根据其优缺点予以评估。

执行摘要

SSAC 不支持目前的《gTLD 注册数据临时规范》快速政策制定流程 (EPDP) 第 2 阶段最终报告[127]（以下简称“最终报告”）。

首先，SSAC 认为，在《通用数据保护条例》(GDPR) 施加的限制范围内，有可能设计出一个更好的系统；而且 EPDP 团队*没有*提供合理且符合安全性和稳定性要求的结果。

其次，最终报告没有提出任何关于承诺完成未解决的章程事项的建议。SSAC 参与并支持 EPDP 第 2 阶段工作的条件是：EPDP 团队承诺对若干第 1 阶段问题进行审核。遗憾的是，EPDP 团队并未审核相关问题，且这些问题仍未解决。

第三，除了上述问题之外，SSAC 还反对以下几项具体建议，即：

- *第 6 项建议：优先级*。将网络安全威胁归类为“第 3 优先级”不足以解决当前严重的网络威胁现实问题。
- *第 10 项建议：确定 SSAD 响应时间的可变 SLA*。SSAC 担心响应时间长会导致 SLA 几乎无法执行，且实施建议可能会使签约方对数据请求的响应日益变得更慢。

[127]请参阅 https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-31jul20-en.pdf。

- *第 12 项建议：披露要求。*SSAC 担心签约方可能会自行决定披露数据请求者的身份，而不是仅在数据保护法要求时才这样做。泄露数据请求者的身份可能会使他们面临危险并妨碍调查。
- *第 14 项建议：财务可持续性。*此项建议包含有缺陷的措辞，不公平地将成本转嫁给受害者，这种表述不符合正常的商业惯例，并且违反了 SSAC 之前向 ICANN 董事会提出的建议。此项建议不是根据 GNSO 程序起草的，没有证据支持，可能不符合 GDPR 要求。

如果更改某些建议，并且如果 GNSO 承诺完成属于《EPDP 章程》的一部分但仍未解决的工作，那么设想在第 2 阶段开发一个非公开注册数据标准化访问/披露系统 (SSAD) 可能会成为改善现状的一种方法。如果 GNSO 能够保证通过正式的政策制定流程立即对自然人与法人、隐私/代理以及数据准确性问题进行审核，那么 SSAC 或许能够支持最终报告。

1 简介

SSAC 本着专业和诚信的精神参与了 EPDP 的工作，在第 1 阶段和第 2 阶段共投入了数千小时的志愿工作，并与 ICANN 社群的一众同事一起勤勉工作。

如 SAC111 所述：

> 和大多数参与者一样，SSAC 在许多问题上做出了妥协，以推动相关工作和访问系统上线。为避免存疑，SSAC 认为现有的第 2 阶段最终报告及其建议远远没有解决 ICANN 职权范围内应该和可能解决的安全性和稳定性问题。SSAC 认为，标准化访问/披露系统 (SSAD) 的初始版本提供数据的方式和速度将无法满足许多业务安全需求。我们认为，在 GDPR 施加的限制范围内，有可能设计出一个更好的系统。如今为了推动相关工作继续进行，SSAC 支持建立一个可以及时改进的坚实基础，而不是主张维持一个理想的系统。[128]

SSAC 支持这一声明。SSAC 不支持目前的第 2 阶段总体结果。

我们认为，在 GDPR 施加的限制范围内，有可能设计出一个更好的系统；而且 EPDP 并没有提供合理且符合安全性和稳定性要求的结果。而且，最终报告没有提出任何关于承诺完成未解决的章程事项的建议。SSAC 参与并支持第 2 阶段的条件是：EPDP 团队承诺对若干第 1 阶段问题进行审核。遗憾的是，EPDP 团队并未审核相关问题，且这些问题仍未解决。

[128]请参阅 SAC111，第 5 页，位于：https://www.icann.org/en/system/files/files/sac-111-en.pdf。

在最终报告的二十二项建议中，SSAC 反对其中四项，即：

- *第 6 项建议：优先级。*将网络安全威胁归类为“第 3 优先级”不足以解决当前严重的网络威胁现实问题。
- *第 10 项建议：确定 SSAD 响应时间的可变 SLA。*SSAC 担心响应时间长会导致 SLA 几乎无法执行，且实施建议可能会使签约方对数据请求的响应日益变得更慢。
- *第 12 项建议：披露要求。*SSAC 担心签约方可能会自行决定披露数据请求者的身份，而不是仅在数据保护法要求时才这样做。泄露数据请求者的身份可能会使他们面临危险并妨碍调查。
- *第 14 项建议：财务可持续性。*此项建议包含有缺陷的措辞，不公平地将成本转嫁给受害者，这种表述不符合正常的商业惯例，并且违反了 SSAC 之前向 ICANN 董事会提出的建议。此项建议不是根据 GNSO 程序起草的，没有证据支持，可能不符合 GDPR 要求。

虽然 SSAC 不反对最终报告中的其他建议，但这并不意味着我们对这些建议都感兴趣。例如，虽然 SSAC 支持 SSAD 认证的想法，因为认证是一种旨在满足 GDPR 要求的保障措施，可为合法请求提供信任和文档，但是，我们不知道认证是否是一个有效的工具。根据拟议的政策，是否披露数据将完全取决于每个注册服务机构和注册管理运行机构的决策，而这些机构的评估方法和标准有很大差异，将会提供不均衡、主观且不可预测的结果。提议的政策可能无法为那些明显合法的请求被拒绝的数据请求者提供有效的追索权。因此，无论实施的认证计划的力度如何，它都可能无法提供任何结果，也可能无法证明数据请求者的诉求是合理的。这不是一个可靠的结果，也达不到 GDPR 允许的水平。[129]

最终报告中的几项建议未能达成共识，遭到了相当多参与机构的正式反对。然而，一些社群成员却声称，GNSO 理事会必须立即对整个最终报告进行一次“同意或反对”表决，也就是说，同意所有建议或反对所有建议二选其一。我们认为，这种“全同意或全反对”的方法会绕过共识流程。它还有可能违反 GNSO 程序，因为其中有这样的表述：“如果最终报告包含 PDP 小组未达成 [原文如此] 共识的建议，GNSO 理事会应商议是否采纳这些建议，或将这些建议保留以供进一步分析和处理。”[130]

[129]2018 年 7 月，欧洲数据保护理事会致函 ICANN 组织并确认“在 WHOIS 系统下处理的个人数据可供拥有合法权益的第三方访问，前提条件是采取了恰当的保障措施以确保披露是适当的，且仅限于披露必要的数据，同时满足 GDPR 的其他要求……”，欧洲数据保护理事会致马跃然的信函，
https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

[130]GNSO 政策制定流程手册，第 13 节“理事会商议”，第 8 页。此程序也适用于 EPDP。
https://gnso.icann.org/sites/default/files/file/field-file-attach/annex-2-pdp-manual-24oct19-en.pdf

我们注意到，虽然这些建议试图创建一个整体计划，但它们之间并没有非常紧密的相互依存关系而需要进行“全同意或全反对”表决。当然还有修改建议的余地。一些建议（当然还有许多子建议中的若干项）可能会被拒绝，而其他建议则依然保持原样。如果没有通过所有建议或者没有通过目前版本的书面建议，整个工作将会瓦解，这是一个错误的想法。GNSO 的程序是这样表述的：“GNSO 理事会可能会采纳最终报告中包含的全部或部分建议”，并且可能会监督修订建议的工作。可能需要 GNSO 理事会和 ICANN 董事会履行其职责，继续努力工作，而且需要他们对工作结果进行审议。ICANN 及其多利益相关方流程的合法性受到广泛关注和严格审核。

本声明的其余内容详细说明了 SSAC 关注的几个重要方面。

2 未完成的章程事项

在 SAC111 中，SSAC 曾提出自己的关切：《EPDP 章程》中的事项没有得到讨论和决策。其中指出，“涉及数据主体的重要问题，包括自然人与法人、隐私/代理服务，以及数据准确性等，面临着被 EPDP 团队忽视的危险。”[131]这些主题在第 1 阶段被推迟处理。SSAC 参与并支持第 2 阶段工作的条件是：EPDP 团队承诺对这些问题进行审核。遗憾的是，EPDP 团队并未审核相关问题，且这些问题仍未解决。例如：

- 最终报告中未提及通过 PDP 审核自然人与法人问题的承诺。
- 最终报告指出：“结论——准确性与 WHOIS 准确度报告体系：根据 GNSO 理事会的指示，EPDP 团队将不会进一步审议这一主题，而是有望成立一个范围界定小组，进一步探讨与准确性和 ARS 相关的问题，以协助确定相应的后续措施来解决已确定的潜在问题。”成立范围界定小组并不是推进任何工作的承诺。这里需要进行 PDP 级别的决策。
- 隐私/代理问题：2016 年代理服务认证问题 (PPSAI) 工作没有解决 GDPR 提出的属于 EPDP 职权范围内的重要问题，并且 PPSAI 工作阶段与 EPDP 工作阶段仍然彼此分离。还需开展更多工作。
    - 有必要讨论受影响的相关方如何向 ICANN 认证的隐私/代理服务提供商（数据控制人）提出访问基础域名联系人数据的请求。能否请求访问注册数据是 EPDP 和 SSAD 的全部要义。最终报告的意思是，ICANN 将所有受隐私/代理服务保护的域都保留在 SSAD 之外，并且也不在其服务水平协议和问责机制之内。

[131]SAC111：SSAC 关于《gTLD 注册数据临时规范》快速政策制定流程第 2 阶段初步报告的意见，2020 年 5 月 4 日，第 8 页。https://www.icann.org/en/system/files/files/sac-111-en.pdf

- 这是属于《EPDP 章程》的事项。《EPDP 章程》中的使命和工作范围一节指出，“EPDP 团队应考虑针对 GNSO 未来工作可以提出哪些必要的辅助建议，以确保重新评估相关的共识性政策（包括与注册数据相关的政策），使其符合适用法律要求。”[132]EPDP 在这个问题上并没有这样做。

自然人与法人问题仍然没有得到解决，部分原因是因无法解释的原因未能及时进行研究。EPDP 第 1 阶段报告建议 ICANN“尽快”开展研究，审议区分法人与自然人的可行性和成本，其他行业和组织如何成功区分法人与自然人，以及区分法人与自然人对注册域名持有人带来的隐私风险（第 17.2 项建议）。[133]2019 年 5 月 15 日，ICANN 董事会接受了该建议，并指示 ICANN 工作人员按照针对 EPDP 第 2 阶段工作的建议执行该项目。[134]

有两个问题：

1. 该研究报告于 2020 年 7 月 8 日提交给 EPDP 团队，*晚于*最终报告完成日期，由于为时过晚，导致无法对法人与自然人议题给予充分的审议。
2. 研究报告没有调查一些最相关和最明显的例子，例如，如何以及为什么在位于欧盟范围内的房地产注册管理机构、公司注册管理机构以及商标注册管理机构中收集和发布自然人数据和法人数据；以及位于欧盟范围之外的此类注册管理机构如何处理居住在欧盟境内的数据主体的数据。虽然该报告指出“大多数欧盟 ccTLD 运营商会继续发布法人注册域名的部分（某些情况下是全部）联系人数据字段的信息”，[135]但该报告没有提供诸如哪些 ccTLD 运营商会发布哪些数据的清单之类的详细信息。

SSAC 要求 GNSO 理事会和 ICANN 董事会解释以下两个问题：为什么这么晚才提交报告，以及为什么没有对预期的受益者（EPDP 中的社群参与者）兑现董事会的决议。为了给今后的决策提供必要的信息，最终可能需要修改报告以提供上述缺失的分析和其他相关信息。

[132]EPDP 团队最终采纳的章程 - 2018 年 7 月 19 日。位于：https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter?preview=/88574674/90767676/EPDP%20FINAL%20Adopted%20Charter%20-%2019%20July%202018.pdf。

[133]https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf。

[134]请参阅 ICANN 董事会决议（2019 年 5 月 15 日），https://features.icann.org/consideration-gnso-epdp-recommendations-temporary-specification-gtld-registration-data，以及附带的 ICANN 董事会平衡记分卡，第 17 项建议，第 5 页，https://www.icann.org/en/system/files/files/epdp-scorecard-15may19-en.pdf

[135]在域名注册数据目录服务中区分法人与自然人。https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20200708/5f72ece1/Rec17.2_Legal-Natural_8jul201-0001.pdf。

如 SAC111 中所述：“GNSO 明确制定了章程，以便 EPDP 工作组和参与者可以了解交付成果。GNSO 制定了工作组标准和程序，旨在以可预测和公平的方式开展工作，同时参与工作组的各个团体应该能够履行对彼此做出的承诺。如果既定流程失败且关键要素问题得不到解决，会威胁到 ICANN 在事关全球利益的关键问题上制定政策的合法性。”[136]

3 与请求优先级排序和响应时间相关的重要问题

这两项建议是紧密结合在一起的，其中第 6 项建议提出了数据披露请求“优先级”的概念，第 10 项建议则非常准确地界定了相关签约方对此类请求的预期响应时间。提出为各种类型的数据披露请求确定不同的优先级处理顺序这样的政策建议是有益的，因为有些数据可能几乎需要立即披露，用于缓解本质上时效性高和/或具有较大影响力的问题，而其他数据则不是紧急迫切的需要披露。同时，向参与披露流程的签约方和其他方提供关于预期的响应时间框架的政策指导（包括请求的状态和请求的数据，如果已获批准的话），对于创建一个兼具一致性和问责制的系统也非常有用。

遗憾的是，由此产生的建议远远超出了所需的政策建议，并且为这些政策规定了非常具体的实施细节。这些细节僵化粗糙且设计不当，无法满足许多最迫切的访问 RDS 数据的需求，尤其是在网络安全领域。尽管用意良好，但将如此详细的实施规划纳入政策，很可能会产生的净效果就是开发一个难以管理的复杂系统，进而不仅因许多不同类别的请求给签约方带来过重的负担，而且不幸地让许多数据请求者在其他类型的请求上享受不到充分的服务。

SSAC 支持确定不同的优先级和预期响应时间框架的高层次目标。但是，具体实施工作应该留给实施团队。实施团队应包括：负责为访问请求提供数据的签约方代表、经常提出数据请求的各方，以及负责管理 SSAD 和监督的 ICANN 工作人员。应由这个团队来确定优先级和响应时间，并且应反映常见用例及其相对紧迫性（从时效性、影响力和/或其他共同商定的因素方面评估）。最终报告内第 6.1.1 项建议中关于第 1 优先级请求的清单为此类讨论提供了一个起点，但该清单并不完整。支持这一框架的最终实施建议应由 GNSO 理事会审核和批准。随着时间的推移，可以使用第 18 项建议中设想的演进机制或最终采用的同等机制来重新审视和调整这些因素。

4 反对关于优先级的第 6 项建议

由于没有提供更好的办法来解决上述优先级和 SLA 问题，SSAC 反对第 6.1 项和第 6.2 项建议。

[136] SAC111：SSAC 关于《gTLD 注册数据临时规范》快速政策制定流程第 2 阶段初步报告的意见，2020 年 5 月 4 日，第 8 页。https://www.icann.org/en/system/files/files/sac-111-en.pdf

将网络安全威胁归类为“第 3 优先级”着实不能解决当今的在线威胁。这些分类未能解决当今发生的一些需要灵活应对的最严重的在线攻击。此类攻击不仅造成了巨大的财务影响，而且通过勒索软件、数据渗漏网络和大规模的敲诈性 DDoS 攻击等方式导致数百万的敏感个人记录遭到在线泄露。还需对分类系统进一步分析，以反映各种不同形式攻击的时效性和影响力。至少，这种系统应提供一个政策框架来指导实际的实施流程，以便根据多个因素解决及时获取数据的需求。如果不更新第 6 项建议来说明需要及时响应各种不同攻击，则需要更严格地限制第 10 项建议（确定 SSAD 响应时间的可变 SLA），要求及时提供数据以便为针对此类攻击做出响应提供支持。SSAC 此前曾在 SAC111 第 3.2 节中进一步概述了这种做法的理由。[137]

5 反对关于确定 SSAD 响应时间的可变 SLA 的第 10 项建议

由于没有提供更好的办法来解决上述优先级和 SLA 问题，因此，SSAC 反对第 10 项建议。虽然这项建议的目标很好，但 SSAC 不支持这项书面建议。这项建议存在逻辑缺陷，它没有提供一个用于响应安全威胁的合理的 SLA。部分原因在于，第 6 项建议（优先级）将安全威胁归类为“第 3 优先级”。[138]这个优先级太低，响应速度太慢，无法解决网络安全事件。[139]

第 1 阶段的 SLA 目标是五 (5) 天。但是，最终报告第 10.11 节却是这样表述的：“在第 2 阶段，签约方针对 SSAD 第 3 优先级请求的合规响应目标是十 (10) 个工作日。”遗憾的是，在第 1 阶段根本没有制定具有约束性的 SLA，包含处罚说明的具有约束性的 SLA 只在第 2 阶段才生效。第 2 阶段 SLA 允许签约方比第 1 阶段的响应速度*更慢*，而不是随着经验的积累变得更快。就实现安全性和稳定性的目标而言，十天太长了。这项建议自预备报告以来一直没有发生重大变化，当时 SSAC 在其发布的 SAC111 第 3.2 节中指出“反对这种矛盾的做法”：

> 这些目标与创建 SSAD 的初衷不一致。网络安全请求往往属于高度优先级事项。本质上，这种做法通常是可操作的，目的就是防止在攻击过程中（例如，恶意软件和网络钓鱼）对多个公众受害者造成持续的有效伤害。运营网络安全请求也没有 URS 请求那么紧迫。而且，SSAD 的总体模型是基于“网络安全请求由认证签约方在问责制系统中提出”这一假设，因此减轻了扩大审核的需要。SSAC 建议，将（由认证签约方提出的）运营安全请求

[137]https://www.icann.org/en/system/files/files/sac-111-en.pdf

[138]除了涉及“迫在眉睫的生命威胁、严重人身伤害、关键基础设施（在线和离线）损坏或剥削儿童”的案件之外。

[139]只有极小比例的安全问题和网络犯罪会达到第 1 优先级处理的高标准，此类事件涉及“迫在眉睫的生命威胁、严重人身伤害、关键基础设施（在线和离线）损坏或剥削儿童”。

移动到第 2 优先级事项中。如果签约方担心网络安全请求的数量，那么在三 (3) 个工作日内做出响应的折中方案是合理的。

随着请求者和签约方增强信心和逐渐提高效率，没有理由响应时间会日益变得越来越长、越来越宽松。因此，从第 1 阶段到第 2 阶段延长了数据控制人必须对任何优先级的请求做出响应的时间（正如 SLA 中定义的那样），这是不合情理的；对于相同优先级的请求，从第 1 阶段到第 2 阶段的响应时间应保持不变或缩短。

SSAC 担心 SLA 几乎无法执行，还担心实施这项建议会带来其他问题。响应时间 SLA 包括所有响应时间的滚动平均值。签约方可以快速拒绝接受所有数据请求，或者也可以立即请求获取所有请求的更多信息。这会让签约方的平均响应时间非常短。然后，这将允许签约方在违反响应时间 SLA 之前，长时间延迟其他请求。第 8.1 项建议没有禁止此类自动操作。因此，ICANN 合规部必须能够确定签约方是否审核了请求并按照第 8 项建议做出了回复。我们不确定 ICANN 组织的工作人员如何确定这一点，因此我们不确定 SLA 是否切实可行。

6 反对关于披露要求的第 12 项建议

第 12.2 项建议将允许签约方随时披露数据请求者的身份，甚至允许将“披露”数据请求者身份作为一项惯例和自动化程序。因此，这项建议可能会超出或违反欧洲数据保护理事会 (EDPB) 给 ICANN 的建议，该建议指出，不必将数据请求者的身份推送给数据主体（注册人）。披露数据请求者的身份将损害调查，可能会危及数据请求者的安全和权利，并且可能会招致对使用第 6 条请求的恐惧，这当然不是 GDPR 的意图。签约方可能需要满足一个平衡测试才能揭示请求者的身份，因为第三方数据请求者是数据主体，并且也拥有 GDPR 规定的权利。

第 12 项建议应禁止签约方披露数据请求人的身份，除非适用法律*要求*披露。我们建议数据控制人遵守法律规定，不逾矩。我们重申 SAC055 和 SAC101v2 中的观点，“SSAC 认为，如果执法部门和安全从业人员出于合法目的需要获取域名责任方的真实身份，则此类访问请求必须符合法律要求。”

ICANN 在 2018 年 5 月 10 日致欧洲数据保护理事会 (EDPB) 的信中提出以下问题：

“a) 注册人或其他第三方是否必须看到提交 WHOIS 查询的个人/实体的身份？”

“b) 注册人或第三方是否必须看到执法机构要求访问非公开 WHOIS 的请求？”

EDPB 的答复如下：

> “通过适当的日志记录机制确保访问的可追溯性，并不是一定要求要将日志信息 [数据请求者的身份] 主动传送（推送）给注册人或第三方。ICANN 和参与 WHOIS 系统的其他控制方有责任确保不向未经授权的实体披露记录信息，特别是以免危害合法的执法活动。”[140]

GDPR 要求数据控制人在提供服务时，通常情况下必须告知数据主体哪些*类型*的相关方可以处理他们的数据。GDPR 并未要求在有人请求访问数据主体的数据时，应主动通知数据主体。GDPR 要求数据控制人仅在*当数据主体请求获取该信息*时，才向数据主体移交第三方数据请求者的身份。

披露数据请求者的身份可能会给签约方带来一些问题。披露数据请求者的身份可能会造成对使用 GDPR 第 6 条请求的偏见和恐惧。它可能会对出于 GDPR 规定的合法目的获取所需数据的做法（例如，缓解网络犯罪、保护受害者，以及可能导致诉讼案件或执法行动的调查）产生严重损害。GDPR 规定中显然还存在以下例外情况：当披露或通知请求者的身份可能会损害一方（例如，第三方请求者）实现其合法目的的能力时，数据主体享有知情权。[141]在调查过程中可能会发生这种情况。[142]

EPDP 团队没有审核这些问题，也没有收到关于这些问题的充分的法律建议。我们想知道数据请求者享有怎样的权利——他们是数据主体，而且他们的数据也受到 GDPR 的保护。为了提出第 6(1)f 条的请求，能否迫使数据请求者向数据主体或数据控制人放弃其隐私权？（GDPR 规定，不得将迫使任何数据主体放弃其隐私权作为合同条件。）签约方告诉数据请求者，签约方已将请求者的身份共享给注册人，因此通知了请求者和注册人双方，这样做是否不公平？

SSAC 曾向 EPDP 团队及其法律咨询小组提出过关于这些问题的疑问，建议将这些问题发送给 Bird & Bird 以征询外部法律建议。但是 EPDP 拒绝了这项请求，并且从未将这些问题发送给 Bird & Bird。因此，从这个意义上说，EPDP 没有充分了解情况，而且允许过度披露请求者身份信息，这种做法不仅不必要，而且是有害的。

7 反对关于财务可持续性的第 14 项建议

SSAC 拒绝接受第 14.2 项和第 14.6 项建议。

[140]EDPB 主席安德里亚 • 耶利内克 (Andrea Jelinek) 致 ICANN 首席执行官马跃然的信函，2018 年 7 月 5 日。https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

[141]GDPR 第 14 条，第 5 段。

[142]信息委员会办公室，“知情权：是否有例外？”https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/#:~:text=There%20is%20no%20automatic%20exception,a%20specific%20exception%20or%20exemption

SSAC 无法接受第 14.2 项建议中的以下措辞：

> 目标是使 SSAD 在财务上自给自足，而不会给注册人带来任何额外费用。数据主体“不得”承担向第三方披露数据的费用；应该主要由 SSAD 数据的请求者承担维护这个系统的费用。而且，在评估 SSAD 用户提交的披露请求后，如果签约方拒绝了此类请求，则数据主体“不得”承担处理数据披露请求的费用。ICANN“可能”会承担维护中央网关的（部分）费用。为了清晰起见，EPDP 团队深知，从根本上说，注册人是 ICANN 大部分收入的来源。这一收入本身并不违反“数据主体‘不得’承担向第三方披露数据的费用”的限制规定。

1) 数据请求者不应主要承担维护系统的成本。[143]请求者当然应该支付获得认证和维护他们对系统的访问权限的费用。但是，目前第 14.2 项建议的措辞却让受害人和辩护人承担系统运营的成本，这是不公平的，并且对互联网安全会有潜在的危险。正如 SSAC 在 SAC101v2 中指出的那样，“一个非免费系统（数据请求者必须为查询付费）可能会使找到和缓解域名滥用所需的查询成本变得非常昂贵，并且在操作上非常困难。”

2) 这个声明不仅影响广泛，而且可能被误解：“数据主体‘不得’承担向第三方披露数据的费用。”然后，使用以下措辞进行了修改：为了清晰起见，EPDP 团队深知，从根本上说，注册人是 ICANN 大部分收入的来源。这一收入本身并不违反“数据主体‘不得’承担向第三方披露数据的费用”的限制规定。

修改后的措辞仍然会阻止注册服务机构在正常的运营活动中将 SSAD 计划的成本转嫁给注册人。签约方通常以履行其核心职责来作为开展业务的成本，并且可能将成本转嫁给客户。[144]但是，第 14.2 项建议禁止这样做。以前的 PDP 都没有保护注册人，使其免于承担与“核心”注册服务相关的成本，或避免将实施共识性政策相关的成本转嫁给他们。以前的 PDP 没有像第 14 项建议中提议的那样试图操纵市场力量的功能。

如果目标仅仅只是禁止注册服务机构在第三方实际请求获取注册人数据时向注册人收取服务费，那么，简单明了地说清除即可。

3) SSAD 不一定要“财政上自给自足”，EPDP 没有提供足够的理由要求这样做。如前所述，[145]SSAC 认为，启动访问 RDDS 数据收费，或未来针对访问 RDDS 数据收费的任何重大变化，必须包含对用户影响以及安全性和稳定性影响的正式评估。

[143]另请参阅第 14.6 项建议。
[144]请参阅 SAC101v2，第 5.4 节。
[145]请参阅 SAC101v2 和 SAC111。

EPDP 团队没有按照要求对相关问题展开研究，也没有按照 GNSO 程序的要求说明政策建议的理由。第 14.2 项建议中的措辞也忽略了 SSAC 向 ICANN 董事会提出的建议，董事会已将该建议转交给 GNSO。所有这些因素导致第 14 项建议不成熟。

2019 年 6 月 23 日，ICANN 董事会审议了 SAC101v2，并将其中的建议提交给 GNSO 理事会审议，以纳入 EPDP 第 2 阶段工作。该建议指出：“启动访问 RDDS 数据收费，或未来针对访问 RDDS 数据收费的任何重大变化，必须包含对用户影响以及安全性和稳定性影响的正式评估，并且应作为正式政策制定流程 (PDP) 的一部分来展开评估工作。”以及：“ICANN 董事会应确保对注册数据政策进行正式的安全风险评估，并将意见纳入政策制定流程。此外，还应针对政策的实施展开单独的安全风险评估。”[146]

从未在任何地方进行过这些对用户影响以及安全性影响的评估。EPDP 团队在没有评估 SSAD 对用户的影响，也没有评估它对 DNS 安全性的影响的情况下，将成本指定给 SSAD 数据请求者的这种做法是不合适的。

当 EPDP 团队提出第 14.2 项建议时，它没有遵循 GNSO 程序，因此这是一项不合理的政策建议。《通用名称支持组织政策制定流程手册》明确指出：“PDP 小组应认真考虑其提议的信息请求和/或由此提出的建议的预算影响、可执行性和/或可行性。”《通用名称支持组织政策制定流程手册》还要求在初步报告中纳入“工作组就有关拟议建议的影响的讨论情况声明，其中包括对经济、竞争、运营、隐私和其他权利、可扩展性和可行性等方面的审议。”

但 EPDP 团队没有审核预算和可实施性对*数据请求者*的影响。EPDP 没有从总体上审核预算和可实施性的影响，只是得到了一个由 ICANN 组织工作人员提供的中央系统启动成本的模糊且没有正式文件记录的估计。EPDP 从未研究过竞争和运营层面的问题，也没有评估收取访问费用将会给安全性和稳定性带来怎样的影响。第 14.2 项建议中的措辞没有经过适当的研究和论证。

在第 14.2 项建议的广泛政策声明之后，最终报告指出，所有细节都应在实施阶段加以处理。任何实施都必须遵循当前第 14.2 项建议中有缺陷且不合理的原则，因此，实施阶段不适合考虑此类基本政策问题。

4) 没有必要强迫数据请求者“主要承担维护系统的成本”。使用 ICANN 资金是一个可行的选择。

[146]董事会 2019 年 7 月 23 日决议，位于：https://features.icann.org/consideration-ssac-advisory-regarding-access-domain-name-registration-data-sac101

SSAD 是 ICANN 社群长期以来设想的一个分层访问系统，是 RDS 系统的一个特征。[147] 注册数据服务始终是签约方作为公共资源提供的一项核心服务。[148]正如多年来所预期的那样，由于法律的变化，现在有必要实行分层/差别化访问。SSAD 将服务于符合公共利益的核心需求。因此，第 14 项建议基本上禁止使用 ICANN 域名注册费来支持系统的运行非比寻常。

使用 ICANN 资金似乎与 ICANN 的使命高度一致。《临时规范》还提醒我们，“ICANN 通常致力于尽最大努力维护现有的 WHOIS 系统”，“ICANN 的使命直接涉及促进第三方数据请求处理，以实现与执法、竞争、消费者保护、信任、安全、稳定、弹性、恶意滥用、主权和权利保护相关的合法和相称的目的。”有关 ICANN 使命和承诺的更多信息，请参阅 SAC101v2，第 5.4 节。[149]

一个类似的例子是集中化域资料服务 (CZDS)，是 ICANN 使用其资金建立和维护的。ICANN 这样做是因为，域文件是各种用户用于合法目的的关键资源。CZDS 不仅有利于用户，也有利于签约方，签约方可以方便地管理域文件订阅。SSAD 也面临着相同的情况，旨在为其数据请求者和签约方提供便利。

5) 下面这句话是最后一刻添加到第 14 项建议中的：“而且，在评估 SSAD 用户提交的披露请求后，如果签约方拒绝了此类请求，则数据主体‘不得’承担披露请求的费用。”不清楚为什么必须增加这些内容，并且这些内容引出了一个问题：是否可以以任何方式将评估数据请求的成本转嫁给注册人，即便是在正常的运营活动中？

6) 建议说：“中央网关‘不得’因数据主体的数据被第三方请求访问或被披露而向数据主体收取单独费用。”我们不清楚中央网关会采用何种方式令人信服地向注册人收费。中央网关与注册人没有任何业务关系。

7) *注册人*的行为通常是导致第三方提交数据请求的原因。

8) SSAC 不知道第 14 项建议是否会违反 GDPR。

第 14 项建议（包括 14.6）设想数据请求者将为提出数据请求付费。收取使用费是实现第 14.2 项和第 14.6 项建议中设想的“成本回收”模型的唯一方法，或者，这是在不将成本转嫁给域名持有人/数据主体的情况下运行系统的唯一方法。

[147]ICANN 社群已经将分层或差异化访问视为注册数据目录服务的一项即将推出的功能。例如，RDAP 协议是专门为提供分层/差异化访问而设计的，因为社群了解到，隐私法可能要求只能与授权用户共享某些类型的数据。现在，SSAD 被视为提供敏感数据的途径（可能会，也可能不会使用 RDAP）。

[148]请参阅 SAC101v2，第 4 页。

[149] https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf

根据 GDPR 规定，如果数据主体想要接收、更新或请求删除其数据，不得向数据主体收取费用。[150]根据 GDPR 的规定，当拥有合法利益的第三方的权利高于数据主体的利益时，前者会收到请求的数据。在 SSAD 中，第三方通常会提出此类请求，因为他们可以提出正当理由，证明数据主体（注册人）侵犯了他们的权利。EPDP 团队没有审核 GDPR 是否允许对第三方数据请求收费，也没有审核在什么情况下允许收费。即使在 SSAC 提议将这一问题发送以征询外部法律建议之后，EPDP 团队也没有就这一问题寻求法律建议。

如果 ICANN 为 SSAD 开发提供资金支持，这个问题是可以避免的。

8 其他意见

以下是关于 SSAC 不反对的其他建议的意见，但仍然可以改进这些建议。我们向 GNSO 提出了以下意见供其审议。

关于第 14 项建议：
第 14.8 项建议有缺陷，而且可能没有必要。其中指出：“在实施和运营 SSAD 时，应避免给较小的运营商带来过重的负担。”我们不相信有人确切地知道“小型运营商负担过重”是什么意思，或者这种措辞的含义是什么。显然，每一个注册服务机构和注册管理运行机构，无论规模大小，都必须使用 SSAD。任何“运营商”使用 SSAD 都可能要花费最低成本。这就是在 gTLD 空间方面开展业务和维持 ICANN 认证的成本。我们担心的是第 14.8 项建议不能被用作一种剥离 SSAD 必要功能的方法。

第 14 项建议的“实施指南”部分也需要进行相应地修订。

第 18.2.3 项建议指出：“常任委员会制定的关于 SSAD 运营和政策的建议必须获得委员会成员的一致同意，才能作为正式建议提交 GNSO 理事会。对于达成一致的共识性建议，**需要获得签约方的支持**。”（着重部分由作者标明）

常任委员会可以提出两种建议：

- 一种是约束合同变更的建议。根据《ICANN 章程》的规定，当由 GNSO 表决时，此类建议必须满足高（绝对多数票）标准。基本上需要签约方的批准才能通过。
- 另一种是实施建议。此类建议不会对签约方产生合同约束力。

[150]请参阅 GDPR 第 15 条、第 57(4) 条，以及信息委员会办公室：https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ 仅在数据主体的请求“明显没有根据或过分”的情况下，GDPR 才允许对数据主体收费。SSAD 不允许且会拒绝接受那些没有任何依据或过分的数据请求。

问题是第 18 项建议将绝对多数票的高标准应用于两种情况，但应该只应用于第一种情况。如前所述，第 18 项建议赋予签约方对实施选项的否决权。据我们所知，赋予任何一方或机构对这种级别的决定的否决权，不是标准的 GNSO 决策流程。[151]

此外，还存在一个实际问题：如果实施问题可以被一两个参与者否决的话，我们不知道支持组织和咨询委员会是否愿意参加常任委员会。

我们不知道，实施问题怎么会上升成为需要获得绝对多数票的 GNSO 指导流程级别的问题。

9 致谢、利益声明、异议、不同观点以及撤回

为了确保公开透明，以下部分为读者提供了有关 SSAC 流程方面的信息。“致谢”部分列出了直接参与本文档撰写的 SSAC 成员、外部专家和 ICANN 工作人员。“利益声明”部分提供了所有 SSAC 成员的个人简介链接，其中包含对可能与成员参与本报告准备工作产生冲突（真实、明显或潜在冲突）的所有利益声明。“异议和不同观点”部分为个人成员提供了一个空间，允许他们描述对本文内容或准备本文过程可能存在的异议或不同意见。“撤回”部分列出了要求不参与本报告中所涉及主题的讨论的个人成员。本文档已得到除“异议和不同观点”以及“撤回”部分中列出的成员之外的所有 SSAC 成员的一致批准。

9.1 致谢

委员会感谢以下 SSAC 成员花费时间和精力来撰写和审核本报告。

SSAC 成员
格雷格 • 亚伦
本尼迪克特 • 阿迪斯 (Benedict Addis)
本 • 巴特勒
史蒂夫 • 克罗克 (Steve Crocker)
詹姆斯 • 加尔文 (James Galvin)
约翰 莱文 (John Levine)
罗德 • 拉斯穆森
塔拉 • 瓦伦

ICANN 员工
安德鲁 • 麦考纳什 (Andrew McConachie)
丹妮尔 • 卢瑟福特 (Danielle Rutherford)

[151]我们不知道，实施问题怎么会上升成为需要获得绝对多数票的 GNSO 指导流程级别的问题。

凯西 • 什尼特 (Kathy Schnitt)
史蒂夫 • 盛 (Steve Sheng)（编者）

9.2 利益声明

以下链接中包含 SSAC 成员的个人简介和利益声明：
https://www.icann.org/resources/pages/ssac-biographies-2019-11-20-en

9.3 异议和不同观点

没有任何异议或不同观点。

9.4 撤回

没有撤回。

附录 F——社群意见

F.1. 征询 SO/AC/SG 社群意见

根据《通用名称支持组织政策制定流程手册》的规定，EPDP 团队应在审议的早期阶段正式征求每个 GNSO 利益相关方团体和选区的意见。同时，还鼓励 EPDP 团队征询其他 ICANN 支持组织和咨询委员会 (SO/AC) 的意见，SO/AC 可能拥有相关问题方面的专业知识、经验或对这些问题感兴趣。因此，EPDP 团队在开始第 2 阶段的审议时，就联系了所有 ICANN 支持组织和咨询委员会以及 GNSO 利益相关方团体和选区，以征询他们的意见。收到了以下各方的回复：

- GNSO 企业选区 (BC)
- GNSO 非商业利益相关方团体 (NCSG)
- 注册管理机构利益相关方团体 (RySG)
- 注册服务机构利益相关方团体 (RrSG)
- 互联网服务提供商和连接提供商选区 (ISPCP)

相关的完整回复声明可在以下位置找到：https://community.icann.org/x/zIWGBg。

收到的所有意见都已添加到初步意见审核工具，并由 EPDP 团队进行了审议。

F.2. “初步报告”公众意见论坛

2020 年 2 月 7 日，EPDP 团队发布了初步报告以征询公众意见。初步报告概述了所讨论的与拟议的非公开 gTLD 注册数据标准化访问/披露系统 (SSAD) 有关的核心问题，并附上了初步建议。

EPDP 团队采用了 Google 表单工具来促进公众意见审核。除了个人提交的两份提案之外，还收到了 GNSO 利益相关方团体、选区、ICANN 咨询委员会、公司和组织提交的 45 份提案。提供的意见位于：https://docs.google.com/spreadsheets/d/1EBiFCsWfqQnMxEcCaKQywCccEVdBc9_ktPA3PU8nrQk/edit?usp=sharing。

为了便于对公众意见进行审核，EPDP 团队开发了一套公众意见审核工具 (PCRT) 和讨论表（请参阅 https://community.icann.org/x/Hi6JBw）。通过在线审核和全体会议，EPDP 团队完成了对已收到的意见的审核和评估，并商定了针对建议和/或报告的修改意见。

F.3. 关于附录的公众意见

2020 年 3 月 26 日，EPDP 团队发布了初步报告附录以征询公众意见。附录涉及的内容主要是 EPDP 团队关于初步建议和/或上文所述第 2 优先级事项的结论。

EPDP 团队采用了 Google 表单工具来促进公众意见审核。除了个人提交的一份提案之外，还收到了 GNSO 利益相关方团体、选区、ICANN 咨询委员会、公司和组织提交的 28 份提案。提供的意见位于：https://docs.google.com/spreadsheets/d/1jN5ThNtmcVJ8txdAGw0ynl5vrGJOuEv8xeccvzjR9qM/edit#gid=2086811131。

为了便于对公众意见进行审核，EPDP 团队开发了一套公众意见审核工具 (PCRT) 和讨论表（请参阅 https://community.icann.org/x/Hi6JBw）。通过在线审核和全体会议，EPDP 团队完成了对已收到的意见的审核和评估，并商定了准备将哪些第 2 优先级事项建议和/或结论纳入本最终报告。

附录 G——法务委员会

提交给 Bird & Bird 的第 2 阶段问题

1. 审议标准化访问/披露系统，其中：

   - ICANN 根据合同要求签约方 (CP) 披露注册数据，包括个人数据，
   - 必须直接通过 RDAP 或通过中间请求认证/授权机构向请求者披露数据，
   - 由 ICANN 委托的第三方执行认证，没有 CP 的参与，
   - 以自动化方式进行披露，无需任何人工的手动干预，
   - 根据 ICANN 的合同要求，CP 应将处理个人数据的目的和实体类型及时告知数据主体。CP 与 ICANN 的合同还要求在数据主体与 CP 签订注册协议之前，CP 应告知数据主体这种潜在的数据披露和第三方数据处理，并且每年通过 ICANN 要求的注册数据准确性提醒进行通知。CP 已经这么做了。

   而且，还假设已采取以下保障措施

   - ICANN 或其指定人员已经确认/验证了请求者的身份，并且要求请求者在每种情况下：
     - 表明其拥有请求和处理数据的法律依据，
     - 提供法律依据，
     - 表明其只请求访问满足其目的所需的数据，
     - 同意按照 GDPR 规定处理数据，并且
     - 同意遵守欧盟标准合同条款来进行数据传输。

   - ICANN 或其指定人员负责记录对非公开注册数据的请求，定期审核这些日志记录，对可疑的滥用行为采取合规措施，并根据数据主体的请求提供这些日志。

   1. 这种情况下，CP 在处理数据披露时可能会面临哪些风险或责任（如果有的话），包括第三方滥用或规避保障措施的风险？

   2. 是否认为上述标准和保障措施足以使注册数据的披露合规？如果存在任何风险，什么样的改进措施或额外的保障措施可消除 [1] 这种风险？

   3. 在这种情况下，CP 是数据控制人还是数据处理人 [2]？CP 的责任在多大程度上（如果有的话）受到这种控制人/处理人的区别的影响？

4. 只回答了 CP 是否仍然存在风险：如果 CP 仍然存在风险，那么根据披露请求的性质，也就是说，根据是否要求提供数据，例如私人请求者提出民事索赔，或执法机构根据其管辖权或犯罪性质（轻罪或重罪）或相关制裁（罚款、监禁或死刑），可能还要采取哪些额外的保障措施来消除 CP 的责任？

脚注 1：“在此，有必要强调保障措施在减轻对数据主体的不利影响方面可能发挥的特殊作用，从而改变权利和利益的平衡，使数据控制人的合法利益不会被践踏。”(https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

脚注 2：https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

2. 当第三方根据认证计划访问非公开 WHOIS 数据时，如果第三方出于规定的目的对数据访问者进行了认证，并承诺遵守类似于数据使用行为准则的某些合理保障措施，但却在处理此类数据时曲解了其预期目的，随后以违背规定目的的方式处理数据，则这种情况下，签约方应承担多少责任（如果有）。在这种情况下，如果签约方可能承担责任，是否可以采取措施来缓解或减轻签约方的责任风险？

3. 假设有一项政策允许已获认证的签约方通过 SSAD 访问非公开 WHOIS 数据（并要求已获认证的签约方承诺遵守类似于行为准则的某些合理保障措施），根据第 6(1)(f) 条的规定，在法律层面是否允许：

   - 定义认证方提出的特定类别的请求（例如，针对恶意软件攻击的快速响应，或联系无响应的知识产权侵权者），对此可以自动提交访问非公开 WHOIS 数据的请求，而无需手动验证每个单独披露请求的认证方是否具备资格，和/或
   - 能够自动披露此类数据，而无需控制人或处理人对每个单独的披露请求进行人工审核。

此外，如果无法实现这些步骤的自动化，请提供关于如何按照第 6(1)(f) 条的规定执行平衡测试的指导意见。

有关信息，请参考以下潜在保障措施：

- 根据 CP 与 ICANN 的合同，必须披露数据（源于 EPDP 第 2 阶段政策）。
- CP 与 ICANN 的合同要求 CP 将处理个人数据的目的和实体类型及时通知数据主体。要求 CP 通知数据主体，以便数据主体在与 CP 签订注册协议之前，有机会选择退出与 CP 的合同，并且每年通过 ICANN 要求的注册数据准确性提醒进行通知。CP 已经这么做了。

- ICANN 或其指定人员已经验证了请求者的身份，并且要求请求者：
  - o 表明其拥有请求和处理数据的法律依据，
  - o 提供法律依据，
  - o 表明其只请求访问满足其目的所需的数据，
  - o 同意按照 GDPR 规定处理数据，并且
  - o 同意遵守标准合同条款来进行数据传输。
- ICANN 或其指定人员负责记录对非公开注册数据的请求，定期审核这些日志记录，对可疑的滥用行为采取合规措施，并根据数据主体的请求提供这些日志。

4. 根据 GDPR 的规定，数据控制人可以根据 GDPR 第 6 1 c 条的要求向主管执法机构披露个人数据，前提条件是执法机构具有根据适用法律制定法律义务的法律权限。某些评论员将“法律义务”解释为仅适用于基于欧盟或其成员国法律的法律义务。

至于数据控制人：

a. 因此，这是否意味着数据控制人不得将 GDPR 第 6 1 c 条的规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？或者，在什么情况下，数据控制人可将 GDPR 第 6 1 c 条的规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？

b. 除了 GDPR 第 6 I f 条的规定之外，数据控制人是否可将任何其他规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？

至于执法机构：

鉴于 GDPR 第 6 1 条的规定，欧洲公共权威机构不得将 GDPR 第 6 I f 条的规定用作在执行任务时处理数据的法律依据，这些公共权威机构需要具备充分的法律依据，才能在另一个法律依据（例如 GDPR 第 6 I c 条的规定）的基础上披露数据。

c. 有鉴于此，非欧盟执法机构能否将 GDPR 第 6 I f 条的规定用作其处理数据的法律依据？在这种情况下，数据控制人能否将 GDPR 第 6 1 f 条的规定用作披露个人数据的法律依据？如果非欧盟执法机构不得将 GDPR 第 6 1 f 条的规定用作其处理数据的法律依据，那么非欧盟执法机构应依靠什么样的法律依据？

- 执行摘要[152]

问题 1 和 2

执行摘要：
EPDP 第 2 阶段团队于 2019 年 8 月 29 日向 Bird & Bird 发送了第一批问题。Bird & Bird 通过三份备忘录回答了这些问题。备忘录 1 已于 2019 年 9 月 9 日交付。备忘录 1 分析了签约方在拟议的标准化访问/披露系统 (SSAD) 中的法律作用、拟议的保障措施是否充足，以及签约方因通过 SSAD 披露数据而承担责任的风险。发送给 Bird & Bird 的问题附在本文档的附录中，并且包含第 1.1 和 1.2 节中的一系列假设，这些假设构成了以下回复的一部分事实基础。

在这些问题的答复中，Bird & Bird 针对控制权指出：

1. 签约方可能是 SSAD 中的数据控制人，因为注册人历来都抱有这样的合理设想：签约方是向第三方披露数据的控制人。很难证明签约方仅服务于 ICANN 组织的利益，尤其是考虑到相关司法判决建议的控制权门槛较低。
2. 如果 EPDP 团队希望推荐一项政策，该政策规定签约方是 SSAD 中的数据处理人，则可以采取相应措施来支持该政策目标。签约方可能对 SSAD 数据处理的关键方面没有任何实质性的影响，例如：(i) 应处理哪些数据；(ii) 处理时长；以及 (iii) 谁有权访问数据。此外，ICANN 组织还需要进行“持续且谨慎的”监督，“以确保处理方完全遵守指示和合同条款”，并努力向注册人阐释，签约方仅代表 ICANN 组织行事（例如，收集 ICANN 组织网站材料、隐私声明、域名注册过程中的信息）。
3. 然而，监管机构最有可能面临的结果和出发点是，签约方是控制人，并且可能与 ICANN 组织一起通过 SSAD 掌握披露注册数据的联合控制权。

关于 SSAD 的保障措施和责任问题，Bird & Bird 提出了以下几点：

4. 考虑到所涉及的司法管辖区数量，以及 SSAD 可能处理的不同类型的请求，Bird & Bird 无法确认假设中所述的标准和保障措施是否会以完全自动化的 SSAD 合规方式披露数据。
5. Bird & Bird 建议 EPDP 团队应审议与以下问题相关的其他保障措施：(i) 法律依据、比例均衡性和数据最小化；(ii) 个人权利；(iii) 国际数据传输；以及 (iv) 安全性。
6. 根据 GDPR 的规定，参与同一数据处理的当事各方对个人和监管机构都负有责任。个人责任是连带的，这意味着参与数据处理的每一方都有可能对数据主体造成的所有损害负责，只是对控制人和处理人的责任界定标准有所不同。监管机构可能会对

[152]待法律委员会签署执行摘要后进行更新

控制人或处理人提起诉讼，目前尚不清楚当有多方参与相同的数据处理时，是否适用连带责任（即，如果其他人负有责任，则不适宜采取强制行动）。

---

1. 签约方是数据控制人还是数据处理人？

控制人

- 签约方是数据控制人还是数据处理人，这个问题会显著影响签约方的责任。(1.4)
- 控制人是指“单独或与他人共同决定处理个人数据的目的和手段的自然人或法人、公共权威机构、执法机构或其他团体。”(2.2)
- 一个实体是否是控制人，这是一个基于“对关键数据处理决策的控制权”的事实认定。不能分配或放弃控制人的角色。(2.3)
- 第 29 条数据保护工作组在 GDPR 生效之前，提供了关于控制人和处理人角色问题的指导意见。EDPB 目前正在修订这项指导意见，预计将在未来六个月内更新。（2.4、2.19）
- 欧洲数据保护理事会的前身，也就是第 29 条数据保护工作组 (WP29) 确定指出，“控制人概念的首要作用是确定谁应负责遵守数据保护规则，以及数据主体如何在实践中行使这些权利。换句话说就是，如何分配各方肩负的责任。”从字面上看，这反映了控制人有责任履行 GDPR 规定的大多数义务；但这句话也暗示了某种程度的监管权宜之计，因为它表明了让某人负责的潜在需要。Bird & Bird 指出，这可能会影响法院或监管机构的做法。(2.4)
- 就 (i) 处理什么数据，(ii) 处理时长，以及 (iii) 谁有权访问数据这些问题做出关键决策（单独或与他人共同）的实体，实际上是数据控制人，而不是数据处理人，因为这几个问题有时被称为数据处理的“关键要素”。(2.6)
- 实体既可以是数据控制人，也可以是数据处理人。在这种情况下，实体既是数据处理人，同时还出于个人目的使用个人数据。(2.7)

处理人

- 处理人是指“代表控制人处理个人数据的自然人或法人、公共权威机构、执法机构或其他团体。”(2.5)
- 第 29 条数据保护工作组指南强调，在确定实体是属于控制人还是处理人时，必须审核“‘一方行使的实际控制权程度、给数据主体留下的印象，以及数据主体基于这种可见性所产生的合理期望’”。(2.5)

- 根据 WP29 的表述，处理人通过“至少在关于处理目的和处理手段的关键要素问题上，执行控制人给出的指示，为其他人的利益服务”。(2.5)
- 处理人只能根据控制人的指示，或 EEA 或其成员国法律的要求来处理个人数据。(2.7)

在 SSAD 中的应用

控制权推定

- 在某些情况下，“通常意味着某种责任的现有传统角色将有助于确定谁是控制人：例如，与雇员数据有关的雇主，与订阅用户数据有关的出版商，与成员或贡献者数据有关的协会”。可采用类似的方法来看待签约方与注册人（或者注册人联系人）之间的关系。(2.8) 同样，“给数据主体留下的印象以及数据主体的合理期望”是确定控制权的重要考虑因素。注册人通常认为签约方是向第三方披露数据的控制人。(2.9)
- 由于签约方目前被视为向第三方披露数据的控制人，这将导致产生这样一种假设：即使实施了 SSAD，签约方仍将是控制人。(2.9)
- 然而，根据对技术处理活动的分析，不能总是做出这样的假设。WP169 确实指出，假设某个人是数据控制人（WP169 中称之为“源于隐含能力的控制权”），则“除非其他因素表明存在相反的情况”，否则这种假设成立。最近的 CJEU 案例——尤其是最近关于时尚标识裁决——也支持开展更接近事实的具体分析。(2.11)

将签约方描述为“代表”其他人行事的难点

- 处理人角色中最重要的元素是：它们只代表控制人行事。很难证明签约方仅服务于 ICANN 的利益，代表 ICANN 处理数据。(2.10)
- 数据披露可能会被视为是签约方的一项不可避免的责任，而不是签约方同意代表 ICANN 这么做。(2.10)

对技术处理活动进行详细的事实分析

- 成为事实上的控制人的门槛（确定数据处理的目的或方式）很低。根据 CJEU 的说法，检验标准只是某人是否“出于个人目的，对个人数据的处理施加影响，并且 (……) 因此参与了数据处理目的和处理手段的决策”。(2.12)
- 在 CJEU 的“耶和华见证会”裁决中，国家耶和华见证会社群组织据说具备“常识”，并且在非常广泛的层面上鼓励和协调社群成员（挨家挨户的传道者）收集数据——尽管如此，它仍被认为满足了与这些社群成员共同拥有控制权的测试资格。在 CJEU 的时尚标识裁决中，网站运营商与 Facebook 平台代码集成就足够了，这样

运营商就可以参与确定 Facebook 的数据收集“方式”，并与 Facebook 一起成为数据的联合控制人。(2.14)

- 因此，法院和监管机构可能会认为签约方参与了数据处理方式的决策，而签约方可能只是实施了/使用了 SSAD。(2.14)

可以支持处理人身份的因素

- 避免控制人身份的关键是能够表明您没有参与确定数据处理的“关键要素”(2.6)。
- 此外，ICANN 对是否按照合规要求披露数据的监控，可成为控制人与处理人关系的一种证明依据，因为“控制人持续和仔细的监督，以确保处理人完全遵守指示和合同条款，这表明控制人仍然完整掌控数据处理操作的唯一控制权。”(2.16)
- 采取措施明确告知数据主体仅代表 ICANN 收集数据（例如，在域名注册过程中披露的信息、年度数据准确性提醒、隐私声明、ICANN 组织网站材料），同时，其他清楚地描述仅由 CP 代表 ICANN 执行此操作的演示文稿可能会使个人更加了解 ICANN 作为控制人的角色，以及签约方作为处理人的角色。(2.17)

总结——签约方最有可能与 ICANN 一起成为联合控制人

- 监管机构最有可能面临的结果和出发点是，签约方是控制人。(2.18)
- ICANN 在确定处理目的和处理方法方面所发挥的作用表明，ICANN 与签约方是向第三方披露数据的联合控制人。(2.18)

2. 拟议的保障措施是否足以使披露注册数据合规？

SSAD 保障措施

- 考虑到所涉及的司法管辖区数量，以及 SSAD 可能处理的不同类型的请求，这种观点无法确认假设中所述的标准和保障措施是否会使完全自动化的系统以合规方式披露数据。(3.8)
- Bird & Bird 指出，在处理个人数据时必须小心谨慎——处理人（违反其与控制人的合同，或违背控制人的指示行事）本身可能会成为控制人，从而面临违规（请参阅备忘录第 7 页的表格）。(3.6)
- 虽然前面所述的保障措施是有帮助的，但还需要纳入以下所述的其他保障措施。(3.8)
    - 法律依据：保障措施需要：(i) 审议签约方，而不仅仅只是请求方，是否拥有处理数据的法律依据；(ii) 说明适用于签约方的特定法律框架；(iii) 如果是

给定情况下的适当法律依据，应确保对合法利益进行相应的平衡测试[153]（并且假设对于某一类请求，利益平衡测试总会支持披露数据，这种设想是不安全的；某些情况下，例如可能会导致死刑的调查或起诉，可能特别成问题）；以及 (iv) 保证不向请求者披露不正确的数据类型或不适当的数据量（例如，基于规则的监控或阻止异常大小的请求、许可系统）。(3.9 - 3.12)

- 个人权利：说明如何处理数据主体请求，包括 (i) 访问日志记录的请求（这种请求本身可能就是高风险的，甚至包含“特殊类别”的个人数据）；(ii) 保留这些日志记录的适当期限；(iii) 向数据主体提供信息的方式；(iv) 如何处理请求者坚持不向数据主体提供信息的情况（例如，出于执法保密要求）；以及 (v) 限制或阻止数据处理的请求。(3.13 - 3.16)

- 数据传输：对于国际数据传输，EPDP 设想遵守欧盟标准合同条款 (SCC) 法律保障机制，但是 (i) 一部分请求者，包括公共权威机构，不同意这些条款；(ii) SCC 中的条款不容易遵守，特别是当进行大规模数据传输时；(iii) 如果欧洲经济区 (EEA) 签约方是数据处理人，则他们不能直接依据 SCC 将数据传输到 ICANN 组织或 EEA 之外的请求者，因此还需要找到相应的解决方法。(3.17)

- 安全性：如果数据受损，安全措施应与数据主体面临的风险相适应。(3.18)

3. 签约方披露数据的责任风险有哪些？

- 如果保障措施不充分或被请求者滥用/规避（或违反了 GDPR 其他方面的要求，例如，未充分通知或缺乏处理数据的法律依据），签约方可能会面临调查、强制令（例如，处理禁令），以及（财务方面的处罚）承担个人民事责任和监管机构的罚款等风险。

- Bird & Bird 针对以下相关问题粗略地指出：(1) 如果双方是联合控制人，这并不意味着双方都必须承担所有的合规要求的责任，(2) 如果 CP 是处理人，则他们只有在不遵守 GDPR 规定的处理方义务，或者超出或违反控制人的合法指示行事的情况下，才会承担第 82 条规定的个人（民事责任），(3) 即使双方被视为联合控制人，近期的法院判决（关于监管机构的执法）也强调指出，联合控制并不意味着对违反 GDPR 的行为承担同等责任，(4) 作为 ICANN 组织的联合控制人，CP 将受益于根据 GDPR 第 26 条的规定，双方必须达成的联合控制权“协议”条款明确规定合理分配各方的责任。

个人责任

- GDPR 第 82 条阐述了关于个人责任的规定。(4.2)

[153]如果欧盟 (EU) 或欧盟/欧洲经济区 (EU/EEA) 成员国法律（包括欧盟或相关成员国为缔约方签订的条约）规定数据披露是一项法律义务，则无需考虑开展合法利益测试。

- 对于因违反 GDPR 的规定在处理数据时造成的损害，应由控制人负责。对于因处理人未遵守特定要求，或者超出或违反控制人的指示行事而在处理数据时造成的损害，应由处理人负责。(4.2)

- 如果证明控制人或处理人与造成的损害事件毫不相关，则控制人或处理人无需承担任何责任。(4.2)

- 如果有多个控制人或处理人参与同一数据处理，则每个实体都对给个人造成的全部损害（共同及连带责任）负责。（4.2、4.3）

- 如果签约方是处理人，则只有当他们未遵守 GDPR 规定的特定于处理人的义务，或者超出或违反控制人的指示行事时，才由签约方负责。在这种情况下，签约方不太可能违反控制人的指示，因为 SSAD 是自动化系统；因此，对他们来说，可能需要承担责任的更大原因是：未充分采取安全措施，或者未遵守 GDPR 关于国际数据传输的规定。签约方可以指望 ICANN 组织来规定安全性和国际数据传输协议条款，赋予签约方声称自己“与造成损害的事件毫不相关”的权利。(4.4)

- 若签约方是控制人且数据披露违反了 GDPR 规定，那么如果他们无法证明自己在积极参与了的数据披露事件中“与造成损害的事件毫不相关”，则不太可能避免要承担个人责任。

- 任何责任都可能导致签约方要承担对数据主体的所有损害的责任。在联合控制人的情况下，这种风险最高。（4.5、4.6）。

- 对数据主体的全部损害负有责任的签约方，可以向其他责任方寻求适当的赔偿。(4.7)

- 签约方和 ICANN 作为联合控制人，承担着积极化解请求者寻求不当访问个人数据的风险的义务。保障措施必须与风险级别相适应。如果请求者规避了 SSAD 保障措施，则法院可能会认为这些保障措施是充分的，这种设想会限制签约方的主要责任。（4.9、4.10）

- 即使是在请求者违反 GDPR 规定的情况下，签约方、ICANN 和请求者均可能被视为“参与了同一数据处理”，各方对违规行为造成的损失负有共同及连带责任。签约方和 ICANN 可能会辩称自己“与造成损害的事件毫不相关”，但在其他情况下，他们需要向请求者寻求成本回收，或在初始诉讼阶段加入请求者以分摊损失。(4.11)

  监管机构的责任

- 监管机构可能会针对控制人或处理人提起诉讼。(4.12)

- 目前尚不清楚在多方参与数据处理的情况下，是否适用共同及连带责任（即，如果其他人负有责任，强制措施可能是不合适的)。(4.13)

- 法律中需要有明确的措辞，以强制实行共同及连带责任——这强化了以下论点：如果是针对监管机构的罚款，则应明确说明需承担的共同及连带责任。第 83(2)(d) 条明确规定，共同及连带责任不适用于监管机构。(4.13.2)
- 即使双方是联合控制人，近期的法院判决（关于监管机构的执法）也强调指出，联合控制并不意味着对违反 GDPR 的行为承担同等责任。(4.13.4)

- 因此，签约方和 ICANN 将受益于联合控制权协议条款明确分配的责任（根据 GDPR 第 26 条的规定，在任何联合控制的情况下，当事方必须达成联合控制权协议）。(4.14)

- 或许可以利用 GDPR 中的“牵头机构”（又称“一站式商店”或“一致性”）条款，确保任何强制措施都是通过 ICANN 组织位于布鲁塞尔的机构进行，而不是直接针对签约方采取措施。这种机制仅适用于跨境处理个人数据的情况（涉及多个 EEA 成员国实体，或对多个 EEA 成员国的数据主体有影响）。(4.15 - 4.17)

- GDPR 中的“牵头机构”条款没有特别提到联合控制权，但指导意见指出，如果 ICANN 组织与签约方将 ICANN 位于比利时的机构指定为数据处理的主要机构（即，做出处理决策的地方），可以最大限度地降低直接对签约方采取强制措施的风险。这是一种新颖却未经测试的方法。(4.15 - 4.20)

—

附录：
法律问题 1 和 2：责任、保障措施、控制人和处理人

在 EPDP 团队审议 SSAD 架构的过程中，出现了关于责任和保障措施的若干问题。为此，第 2 阶段法律委员会向外部律师事务所提出了以下问题：

1. 审议标准化访问/披露系统，其中：
    - ICANN 根据合同规定要求签约方 (CP) 披露注册数据，包括个人数据，
    - 必须直接通过 RDAP 或通过中间请求认证/授权机构向请求者披露数据，
    - 由 ICANN 委托的第三方执行认证，没有 CP 的参与，
    - 以自动化方式进行披露，无需任何人工的手动干预，
    - 根据 ICANN 的合同要求，CP 应将处理个人数据的目的和实体类型及时告知数据主体。CP 与 ICANN 的合同还要求在数据主体与 CP 签订注册协议之前，CP 应告知数据主体这种潜在的数据披露和第三方数据处理，并且每年通过 ICANN 要求的注册数据准确性提醒进行通知。CP 已经这么做了。

而且，还假设已采取以下保障措施

- ICANN 或其指定人员已经确认/验证了请求者的身份，并且要求请求者在每种情况下：
  - 表明其拥有请求和处理数据的法律依据，
  - 提供法律依据，
  - 表明其只请求访问满足其目的所需的数据，
  - 同意按照 GDPR 规定处理数据，并且
  - 同意遵守欧盟标准合同条款来进行数据传输。
- ICANN 或其指定人员负责记录对非公开注册数据的请求，定期审核这些日志记录，对可疑的滥用行为采取合规措施，并根据数据主体的请求提供这些日志。

a. 这种情况下，CP 在处理数据披露时可能会面临哪些风险或责任（如果有的话），包括第三方滥用或规避保障措施的风险？

b. 是否认为上述标准和保障措施足以使注册数据的披露合规？如果存在任何风险，什么样的改进措施或额外的保障措施可消除[154]这种风险？

c. 在这种情况下，CP 是数据控制人还是数据处理人[155]？CP 的责任在多大程度上（如果有的话）受到这种控制人/处理人的区别的影响？

d. 只回答了 CP 是否仍然存在风险：如果 CP 仍然存在风险，那么根据披露请求的性质，也就是说，根据是否要求提供数据，例如私人请求者提出民事索赔，或执法机构根据其管辖权或犯罪性质（轻罪或重罪）或相关制裁（罚款、监禁或死刑），可能还要采取哪些额外的保障措施来消除 CP 的责任？

2. 当第三方根据认证计划访问非公开 WHOIS 数据时，如果第三方出于规定的目的对数据访问者进行了认证，并承诺遵守类似于数据使用行为准则的某些合理保障措施，但却在处理此类数据时曲解了其预期目的，随后以违背规定目的的方式处理数据，则这种情况下，签约方应承担多少责任（如果有）。在这种情况下，如果签约方可能承担责任，是否可以采取措施来缓解或减轻签约方的责任风险？

[154] “在此，有必要强调保障措施在减轻对数据主体的不利影响方面可能发挥的特殊作用，从而改变权利和利益的平衡，使数据控制方的合法利益不会被践踏。” https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf

[155] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

问题 3

执行摘要：

EPDP 第 2 阶段团队于 2019 年 8 月 29 日向 Bird & Bird 发送了第一批问题。Bird & Bird 通过三份备忘录回答了这些问题。备忘录 2 于 2019 年 9 月 10 日交付，分析了关于如何在 SSAD 中应用 GDPR 第 6(1)(f) 条所要求的合法权益“平衡测试”的问题，要么采用高度自动化的方式进行平衡测试（问题 A），或者，如果不可能实现此类决策的自动化，则应如何进行平衡测试（问题 B）。本摘要的附录 A 中提供了完整的问题，同时还包含一系列假设，这些假设构成了以下回复的一部分事实基础。

在回答问题 A 时，Bird & Bird 在自动化决策方面指出：

1. EPDP 团队所描述的高度自动化的流程相当于完全自动化的决策，对数据主体具有法律效力或类似的重大影响（“数据主体”在此将成为非公开 gTLD 数据请求的目标）。
2. 一般不允许这样做，除非 GDPR 第 22(1) 条规定的有限法律依据/豁免条款证明数据披露是合理的。这比 GDPR 第 6(1)(f) 条规定的适用范围窄得多。拟议的 SSAD 将很难满足 GDPR 第 22(1) 条的豁免要求；因此，必须首先精心设计 SSAD 结构，使其不属于第 22 条规定的范围。
3. 为了实现这个目标，有必要将自动访问/披露限制在不会对数据主体产生法律或类似重大影响的程度。备忘录中提供的示例包括：针对恶意软件攻击或侵犯知识产权的行为，发布非自然人注册人的管理联系人详细信息。更高风险请求的处理流程不应完全自动化；应该有一些有意义的人为参与（至少是监督）。
4. 或者，可以对 SSAD 结构进行潜在的调整，使其不会基于与请求目标有关的个人数据自动化处理来做出决定。例如，SSAD 可公布其将接受的请求类别，并要求请求者确认自己提出的请求符合相关标准。相反，通过要求*请求者*进行必要的分析并向 SSAD 证明分析结果，SSAD 可能不会基于与请求目标有关的个人数据自动化处理来做出决定（发布数据），因此 GDPR 第 22 条将不适用。但是，依赖请求者的自我证明可能会为请求者滥用该系统创造条件，这（正如之前的回答所阐述）可能意味着 ICANN 和签约方需承担一定的责任。
5. 关于对请求者的身份验证（与评估请求的依据或其他参数截然不同的步骤），Bird & Bird 认为，当然可以通过自动化流程来验证请求者的身份。也可以自动执行请求流程的其他方面。

在回答问题 B 时，Bird & Bird：

1. 阐述了欧盟（第 29 条数据保护工作组）关于如何进行第 6(1)(f) 条规定的合法利益平衡测试的官方指导意见；

2. 指出如果 ICANN 与签约方是联合控制人，则双方都必须确立处理流程中存在的合法利益。就签约方而言，相关利益很可能是第三方（请求者）的利益。相比之下，ICANN 可能能够确立其在确保域名系统的安全性、稳定性和弹性方面的利益*以及*第三方请求者的利益；以及
3. 就可以部署的保障措施进行了高级别讨论，以便进一步扭转支持将数据处理作为 SSAD 组成部分这种设想的局势。

1. 问题 A

问题 A 提出：GDPR 第 6(1)(f) 条（处理的“合法利益”法律依据）是否允许 SSAD 自动处理请求（至少在某些预先确定的请求类别中），而不需要人工逐一 (i) 验证请求是否符合相关的披露标准；以及 (ii) 披露相关注册数据。

SSAD 可能属于 GDPR 第 22 条规定的范围，而不是仅仅只与 GDPR 第 6(1)(f) 条有关

- GDPR 第 6(1)(f) 条允许自动化处理，*除非*这相当于对数据主体具有法律或类似重大影响的“自动化个人决策”（完全自动化的决策），除非 GDPR 第 22(1) 条规定的有限法律依据/豁免条款证明数据披露是合理的，否则一般不允许这样做。

- 虽然 GDPR 第 22 条规定数据主体“有权不服从”此类决定，但在实践中，监管机构将第 22 条解释为一项一般*禁令*（即，数据主体无需反对此类决定）。

- EPDP 团队所描述的决策流程相当于此类可能会影响请求目标的自动化决策（例如，当执法部门希望对运营非法网站的个人提起诉讼时）。

- 如果第 22 条适用于 EPDP 所述的处理，即，**如果 SSAD 处理相当于具有法律或类似重大影响的自动化个人决决，则根据 GDPR 第 6(1)(f) 条（处理的“合法利益”依据）的规定，这种做法是不允许的。**第 22(1) 条规定了比用作第 22 条所述决策依据的更多限制的理由。

- Bird & Bird 指出，**SSAD 将很难满足第 22(1) 条的豁免要求；因此，EPDP 应确保 SSAD 处理流程不属于第 22 条规定的范围。**

缓解策略 1：如果决策可能对数据被披露的个人产生“法律效力或类似的重大影响”，则避免做出自动化决策

- 实现这一目标的一种方法是：将自动访问和披露限制在不会对数据主体产生“法律或类似重大影响”的程度。

- 通过 SSAD 发布数据这个决定本身不会对数据主体产生“法律效力”。与 SSAD 更相关的测试是“类似重大影响”。它是指类似具有法律效力的内容，值得关注的内容（例如，显著影响相关个人的情况、行为或选择）。[156]

- 有可能能够确定不会对个人产生“法律或类似重大影响”的请求类别，例如发布非自然人（公司/组织/机构）注册人的管理联系人详细信息。涉及自然人注册人的其他数据披露更有可能会产生“类似重大影响”。需谨慎处理此类分析。

- 对于更有可能产生“重大影响”的决策，有必要进行人工审核或监督。“标记”人为参与是不够的。为了使人工审核发挥作用，控制人必须确保由有权力和能力改变决策的人进行有意义的监督。

缓解策略 2：避免将 SSAD 设计成包含关于请求目标的个人数据处理，以决定是否遵守请求

- 此外，也有可能调整 SSAD 结构，使其不会陷入“完全基于自动化处理的决策”。GDPR 第 22 条要求做出的决定是基于对*个人数据*的处理。如果是基于除个人数据处理之外的其他内容做出决定，则 GDPR 第 22 条不适用。

- 因此，不应是 SSAD 要求请求者提供详细信息（例如，关于请求目标的信息，例如，注册人是谁，以及为什么需要注册人的数据），然后（自动）分析该信息以评估是否符合发布非公开注册数据的相关标准，而应是 SSAD 公布其将接受的请求类别，并要求请求者确认自己提出的请求符合相关标准。在这种情况下，SSAD 不会处理与请求目标有关的*个人数据*以做出发布数据的决定，因此第 22 条不适用。

- 正如前面提到的问题所述，SSAD 的相关方有责任采取“适当的技术和组织措施”，以防范请求者滥用 SSAD 系统的风险。

- 因此，依赖自我证明而不是评估请求的任何决定都需要对照这些风险缓和义务进行权衡考量；这可能会缩小可以采用这种自我证明方法的使用场景。Bird & Bird 指出，在这种方案下，SSAD 仍然会*出于审核目的*要求请求者提供关于其请求性质的其他信息，但不会将这些信息用于评估请求本身（即，不会用于自动化决策流程）。

2. 问题 B

在这个问题中，**EPDP 团队询问了关于如何进行第 6(1)(f) 条规定的平衡测试的指导意见（假设无法自动执行上述步骤）。**

- 官方指导意见是平衡测试应分为四个步骤：

    1. 评估处理流程要满足的利益要求

[156]根据官方指导意见，以下是可能会产生足够重大影响的决定的经典示例：(i) 影响某人财务状况的决定；(ii) 影响获得卫生健康服务的决定；(iii) 拒绝提供就业机会或使某人处于严重不利地位的决定；(iv) 影响某人受教育机会的决定。

2. 考虑对数据主体的影响
3. 进行临时平衡测试
4. 考虑部署的额外保障措施可能带来的影响，以防对数据主体造成任何不当影响。

1. 评估控制人的合法权益

- 第 6(1)(f) 条规定，如果“处理必需是为了满足控制人或第三方追求的合法利益”，则您可以合法地处理。
- 这个问题包含三个子元素：(i) 合法性；(ii) 是否存在利益；以及 (iii) 必要性。

合法性

- “合法性”似乎不是一项高要求——第 29 条数据保护工作组曾指出“只要控制人按照数据保护法规和其他法律规定的方式追求该利益，就可被视为合法利益。”

确定处理流程中的“利益”

- Bird & Bird 指出，如果 ICANN 与签约方是联合控制人，则双方都必须确立处理流程中存在的合法利益。就签约方而言，相关利益很可能是第三方（请求者）的利益。相比之下，ICANN 可能能够确立其在确保域名系统的安全性、稳定性和弹性方面的利益以及第三方请求者的利益。
- “利益”和“目的”不是一回事。
    - “目的”是处理数据的具体原因
    - “利益”是一种更宽泛的概念，可能是控制人在处理流程中拥有的利害关系，或控制人可从处理流程中获得的利益，或社会可从处理流程中获得的利益。（这也意味着可能是公共利益或个人利益；例如，在采取措施防范商标侵权的情况下，可能是出于个人利益，保护商标免受侵害的个人的合法利益，也可能是出于公共利益，避免公众对商标侵权产生混淆。可以在平衡测试的文档中记录这个因素，它可能会有用。）
- 利益必须是“真实且具体的”，而不应是“模糊和推测的”。
- 在第 25 页，WP217 提供了一份可能引起合法利益问题的背景概述的不完全清单，包括：
    - “行使言论或信息自由权，包括在媒体和艺术领域”
    - 执行法定索赔权

- 防范欺诈、滥用服务，
- 物理安全、信息技术和网络安全
- 用于研究目的的数据处理

- EPDP 建议，潜在的 SSAD 保障措施可以包含：要求请求者表明其拥有提出请求的法律依据，并且能够“提供相应的法律依据”。然而，如果根据第 6(1)(f) 条的规定公布数据，那么这将更有助于请求者确认其接收个人数据的*利益*所在。

必要性

- 关于必要性，Bird & Bird 建议，拟议的处理（披露）必须是为了满足合理利益所“必需的”。
  - 奥地利广播电视公司 (CEJU Oesterreichischer Rundfunk) 案例将其定义为：*“…形容词‘必需的’…意味着涉及到‘紧迫的社会需要’，并且所采取的措施‘与所追求的合法目标相称’。”*
  - 英国一家上诉法院同样认为，必要即表示“超过期望，但还没有到必不可少或绝对必要的程度。”
- Bird & Bird 指出，考虑必要性的一个相关因素可以是：请求者是否试图以任何其他方式（尽管这种做法在执法请求的情况下可能并不合适）与个人联系。
- Bird & Bird 指出，SSAD 提议要求请求者确认他们只请求访问符合其目的所必需的数据。

2. 评估对个人的影响

- Bird & Bird 指出，EDPB 建议在评估对个人的影响时要考虑多种因素：
  - ***对影响进行评估。***考虑对数据主体的直接影响以及数据处理可能产生的更广泛的后果（例如，引发法律诉讼）。
  - ***数据的性质。***考虑数据的敏感性级别以及数据是否已经公开可用。
  - ***数据主体的身份地位***。考虑数据主体的身份地位是否会增加他们的受攻击性（例如，儿童或其他受保护的群体）。
  - ***处理范围。***考虑数据是会被严格保留（较低风险），还是会被公开披露，供大量人员访问，或者是与其他数据相结合（较高风险）。
  - ***数据主体的合理预期***。考虑数据主体是否会合理地期望采用这种方式处理/披露其数据。

- ***控制人与数据主体的身份地位。***考虑协商能力，以及控制人与数据主体之间的任何权限不平衡。

- SSAD 或许可能会考虑这些因素，通过识别会对个人构成高风险的请求来增加对这些请求的关注。
- 可采用一种经典的方法（审视严重性和可能性）来评估风险。
- 这不是纯粹的量化练习；虽然请求的指标（例如，受影响的数据主体的数量）是相关的，但它不是决定性因素，仍然应该考虑请求对单个数据主体的潜在重大影响。

3. 暂时平衡

- 综合考虑控制人或第三方的合法利益与个人的合法利益才可能实现各方的利益平衡。确保履行其他数据保护义务有助于实现平衡，但不具有决定性作用（例如，SSAD 确保与请求者就适当的数据保护制定标准合同条款是有帮助的，因为这可能会降低个人面临的风险，但它不是决定性因素）。

4. 额外保障措施

- Bird & Bird 指出，如果不清楚如何实现平衡，控制人可以考虑采取其他保障措施来减少数据处理对数据主体的影响。
- 例如，额外保障措施包括：
    - 提高透明度
    - 增强数据主体访问或传输数据的权限
    - 无条件选择退出的权利
- WP217 第 41-42 页提供了更多关于保障措施的详细信息，这些保障措施有助于“扭转局势”，即，在合法权益平衡测试中支持数据处理（此处，还包括支持数据披露）。

附录：法律问题 3：合法权益以及自动提交和/或披露

a) 假设有一项政策允许已获认证的签约方通过适用于第三方获取非公开注册数据的标准化访问/披露系统 (SSAD) 来访问非公开 WHOIS 数据（并要求已获认证的签约方承诺遵守类似于行为准则的某些合理保障措施），根据第 6(1)(f) 条的规定，在法律层面是否允许：

- 定义认证方提出的特定类别的请求（例如，针对恶意软件攻击的快速响应，或联系无响应的知识产权侵权者），对此可以自动提交访问非公开 WHOIS 数据的请求，而无需手动验证每个单独披露请求的认证方是否具备资格，和/或

- 能够自动披露此类数据，而无需控制人或处理人对每个单独的披露请求进行人工审核。

b) 此外，如果无法实现这些步骤的自动化，请提供如何按照第 6(1)(f) 条的规定执行平衡测试的指导意见。

有关信息，请参考以下潜在保障措施：

- 根据 CP 与 ICANN 的合同，必须披露数据（源于 EPDP 第 2 阶段政策）。
- CP 与 ICANN 的合同要求 CP 就关于处理个人数据的目的和实体类型及时通知数据主体。要求 CP 通知数据主体，以便数据主体在与 CP 签订注册协议之前，有机会选择退出与 CP 的合同，并且每年通过 ICANN 要求的注册数据准确性提醒进行通知。CP 已经这么做了。
- ICANN 或其指定人员已经验证了请求者的身份，并且要求请求者：
  - 表明其拥有请求和处理数据的法律依据，
  - 提供法律依据，
  - 表明其只请求访问满足其目的所需的数据，
  - 同意按照 GDPR 规定处理数据，并且
  - 同意遵守标准合同条款来进行数据传输。
- ICANN 或其指定人员负责记录对非公开注册数据的请求，定期审核这些日志记录，对可疑的滥用行为采取合规措施，并根据数据主体的请求提供这些日志。

问题 4

执行摘要：

EPDP 第 2 阶段团队于 2019 年 8 月 29 日向 Bird & Bird 发送了第一批问题。Bird & Bird 通过三份备忘录回答了这些问题。备忘录 3 于 2019 年 9 月 9 日发布，分析了有关法律依据的问题，根据这些法律依据，可向数据控制人管辖区范围之外的执法机构披露 gTLD 注册数据中所包含的个人数据。

具体而言，备忘录回答了以下问题：

- 数据控制人是否可以将 GDPR 第 6(1)(c) 条的规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？
- 如果不可以，除了 GDPR 第 6(1)(f) 条的规定之外，数据控制人是否可将任何其他规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？
- 非欧盟执法机构能否将 GDPR 第 6(1)(f) 条的规定用作其处理数据的法律依据？在这种情况下，数据控制人能否将 GDPR 第 6(1)(f) 条的规定用作披露个人数据的法律依据？如果非欧盟执法机构不得将 GDPR 第 6(1)(f) 条的规定用作其处理数据的法律依据，那么非欧盟执法机构应依靠什么样的法律依据？

总的来说，Bird & Bird 建议：

1. 若要适用第 6(1)(c) 条的规定，必须有“控制人必须遵守其规定的欧盟或成员国法律”，因此，在执法机构位于控制人管辖区范围之外的情况下，这一理由的适用范围有限。
2. 在处理个人数据的六项法律依据中，第 6(1)(a) 条 - 同意、第 6(1)(b) 条 - 合同、第 6(1)(d) 条 - 重要的个人利益，以及第 6(1)(e) 条 - 公共利益或权威机构不太可能适用于执法机构的请求。
3. 在非欧盟执法机构请求从欧盟境内的控制人处获取个人数据的情况下，“第 6(1)(f) 条 - 合法权益”可作为控制人的适用法律依据。
4. 如果执法机构位于欧洲经济区之外，则根据 GDPR 规定处理数据的法律依据就无关紧要，因为这些执法机构不受 GDPR 的约束。向欧洲经济区之外的执法机构披露信息的组织，仍然需要具备一个披露信息的有效法律依据，这在 ICANN 的数据披露案例中通常是指合法权益。
5. 如果 CP 受 GDPR 的约束但位于欧洲经济区之外，它们还将受到当地法律的约束。这意味着控制人可能会面临法律冲突。

1. 数据控制人是否可以将 GDPR 第 6(1)(c) 条的规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？

- 仅在欧盟或成员国法律明确规定了法定义务的情况下，控制人才需遵守法定义务以满足必要的数据处理合规要求。
- 如果控制人须遵守欧盟以外司法管辖区法律规定的披露义务，控制人不得将第 6(1)(c) 条的规定用作法律依据。
- 根据欧盟或成员国法律的规定，控制人拥有向非欧盟执法机构披露个人数据的法定义务。
- 双边司法协助条约 (MLAT) 规定，如果收到存在 MLAT 的请求，则控制人应拒绝该请求并参考 MLAT 的要求。如果不存在 MLAT 或其他协议，控制人需要确保向第三国披露数据不会违反当地法律。

2. 除了 GDPR 第 6(1)(f) 条的规定之外，数据控制人是否可将任何其他规定用作法律依据，向数据控制人管辖区范围之外的执法机构披露个人数据？

- 第 6(1)(f) 条和第 6(1)(c) 条的规定可能适用，但其他五项法律依据可能不适用于处理个人数据。
- 在非欧盟执法机构请求从欧盟境内的控制人处获取个人数据的情况下，控制人也许能够展现在披露数据方面拥有（第 6(1)(f) 条中规定的）合法权益。EDPB 也在致 ICANN 的信函中建议采用这种方法（例如，EDPB-85-2018）。

3. 非欧盟执法机构能否将 GDPR 第 6(1)(f) 条的规定用作其处理数据的法律依据？在这种情况下，数据控制人能否将 GDPR 第 6(1)(f) 条的规定用作披露个人数据的法律依据？如果非欧盟执法机构不得将 GDPR 第 6(1)(f) 条的规定用作其处理数据的法律依据，那么非欧盟执法机构应依靠什么样的法律依据？

- 作为国家/地区的实体，执法机构享有国家豁免权益，因此非欧盟执法机构不受 GDPR 管辖约束。
- 即使假设 GDPR 适用于非欧盟执法机构，欧盟地区之外的执法机构似乎也不大可能会考虑证明其根据 GDPR 的规定处理数据是合理做法。
- 因此，非欧盟执法机构无需评估其处理数据所依靠的 GDPR 法律依据。
- 尽管如此，将数据传输到欧盟地区之外的执法机构的控制人仍然需要考虑如何履行第五章（向第三国家/地区或国际组织传输个人数据）中所述的义务。

问题 5（假名化电子邮件地址）

小组讨论了一种选项：将数据主体提供的电子邮件地址替换为本身无法识别数据主体身份的备用电子邮件地址（例如：sfjgsdfsafgkas@pseudo.nym）。讨论中提到了采用此方法的两种选项：(a) 数据主体在多次注册中使用相同的唯一字符串（“假名化”），或者 (b) 每次注册都使用唯一字符串（“匿名化”）。如果采用选项 (a)，则通过交叉引用字符串所用于的所有域名注册的内容，可能（但不一定）会识别数据主体的身份。

这些选项也带来了以下问题：如果采用选项 (a) 和/或 (b)，是否必须将备用地址视为 GDPR 规定的属于数据主体的个人数据？关于在注册目录服务 (RDS) 的公共可访问部分中发布该字符串的拟定建议，这项决定可能会产生怎样的法律后果和风险？

Bird & Bird 给出的总结性回复

我们认为，仍应将选项 (a) 或 (b) 视为在网上发布个人数据。第 29 条数据保护工作组 2014 年在关于匿名化技术的意见 [ec.europa.eu] 中所做的声明似乎提到过这种情况：“如果数据控制人没有删除事件级别的原始（可识别）数据，并且数据控制人移交了该数据集的部分数据（例如，在删除或屏蔽可识别数据之后），则由此得到的数据集仍然是个人数据。”使该电子邮件地址（即使它被屏蔽）可用的目的，也许是为了允许第三方直接联系数据主体（例如，向他们送达法院传票、要求撤销起诉等）。因此，至少在 ICANN/签约方看来，它与该特定数据主体有着非常明确的联系。然而，这两种选择均不被视为是有价值的隐私增强技术 (OPET)/隐私设计措施。

问题 6（同意）

法人注册人提交的注册数据可能包含自然人的数据。第 1 阶段备忘录指出，如果通过采取进一步措施确保注册人指定数据的准确性来减轻风险，则注册服务机构可以依靠注册人自我识别为法人或自然人。该备忘录的后续问题：与此类指定相关的同意选项和要求是什么？具体而言：数据控制人是否有权依赖一份声明，强制要求法人注册人征得自然人的同意（该自然人将充当联系人并且其信息会在 RDS 中公开显示）？如果是，在这种情况下，什么样的陈述（如果有）将有助于控制人从法人注册人那里征得同意？

作为您分析的组成部分，请务必参考 GDPR 政策以及互联网协议（IP 地址）注册管理机构 RIPE-NCC（位于荷兰的欧洲注册管理机构）的做法。RIPE NCC 的客户（注册人）是指在 WHOIS 中公开显示的法人。RIPE NCC 规定其法人注册人有责任获得自然人的许可，并为此提供程序和保障措施。RIPE NCC 陈述的使命理由和数据收集目的类似于 ICANN《临时规范》中的内容。类似的政策和程序可以在 ICANN 内部使用吗？

另请参阅北美 IP 地址注册管理机构 ARIN 的政策。ARIN 有一些欧盟地区的客户。ARIN 还会在 WHOIS 输出中公布自然人的数据。ARIN 的客户是自然人，他们会提交自然人联系信息。

Bird & Bird 给出的总结性回复

本文档分析了 GDPR 规定的同意要求，并审核了同意选项，以便在 RDS 中发布由法人注册人提供的个人数据。

同意要求

根据 GDPR 的规定，必须自由、具体，知情且明确地给予同意。此外，还需要在处理数据之前征得个人同意。控制人必须能够证明已经征得个人的有效同意，并且个人有权随时撤回同意。根据 GDPR 的规定，控制人承担征得同意的义务。控制人可指示第三方代表其征得个人的同意；但是，这样做并不会解除控制人应负的 GDPR 义务。

同意选项

根据上述要求，本文档研究了用于征得同意在 RDS 中公开个人数据的下列选项，并列出了每种选项的合规考虑因素：

1. 控制人直接征得个人的有效同意
    - 在 RDS 中公开个人数据是一个可选选项。
    - 在公开个人数据之前，控制人应根据 GDPR 的规定，直接联系个人以征得个人的同意。
    - 如果个人拒绝同意或未作出回应，将不公开个人数据。

2. 注册人征得个人的有效同意并向控制人提供相关证据
    - 在 RDS 中公开个人数据是一个可选选项。
    - 在公开个人数据之前，控制人要求注册人：(a) 征得个人同意，并 (b) 向控制人提供已征得个人同意的证据。
    - 如果个人拒绝同意或未收到相关证据，将不公开个人数据。

3. 注册人征得个人的有效同意，控制人与个人确认这一点
    - 在公开个人数据之前，控制人要求注册人：(a) 征得个人同意，并 (b) 向控制人提供已征得个人同意的证据。
    - 控制人直接跟进个人：控制人通知个人，注册人已确认其已征得同意。

4. 注册人承担征得同意的义务。
    - 允许注册人提供非个人的联系方式。
    - 默认情况下，注册数据会公开（无论是否包含个人数据）。
    - 注册人通过声明承诺，如果选择提供个人数据，将确保征得个人同意。

问题 7（准确性）

问题 1a

谁有资格援引准确性原则？据我们所知，准确性原则的宗旨之一是保护数据主体免遭因处理不准确信息而带来的损害。其他方（例如签约方、作为控制人的 ICANN、执法机构、知识产权持有人等）是否有资格援引 GDPR 的准确性原则？在回答这个问题时，能否请您明确阐述我们通常应考虑哪些相关方/利益，尤其是在解释之前备忘录中提到的以下段落时：

- 两份备忘录都在几个部分中提到了“相关方”。“相关方”是仅限于控制人？还是我们也应该考虑第三方的利益？
    - “可能会有这样的问题，即，注册域名持有人或账户持有人是否足以确认与技术和行政联系人有关的信息的准确性，而不是直接询问此类联系人的信息。GDPR 没有强制要求，在必须验证个人数据的情况下，由数据主体自行验证。如果合理的话，ICANN 和相关方可能会依靠第三方来确认个人数据的准确性。因此，我们认为没有直接的理由表明目前的程序是不足的。”（着重部分由作者标明）（第 19 段 - 准确性）
    - “总之，因为符合准确性原则是以合理标准为基础，因此，ICANN 和相关方更适合评估这些程序是否足够。从我们的角度来看，由于程序确实需要有助于确认准确性的肯定性步骤，除非有理由认为这些步骤不充分，否则我们认为没有明确的要求对其进行审核。”（着重部分由作者标明）（第 21 段 - 准确性）
    - “如果相关方没有理由怀疑注册人自我识别的可靠性，那么他们可能将在没有独立确认的情况下仅依靠注册人的自我识别。但是，我们也理解，相关方可能会担心部分注册人无法理解这个问题并错误地完成自我识别。因此，如果相关方不采取进一步措施来确保注册人指定数据的准确性，那么自我识别将存在一定的责任风险。”（着重部分由作者标明）（第 17 段 - 法人与自然人）

    1.b 同样，法人与自然人备忘录提到了数据“重要性”在确定付出怎样的努力以确保数据准确性这个问题上的作用。对数据“重要性”的评估是否仅限于考虑数据对数据主体和控制人的重要性？还是也会考虑数据对第三方（在这种情况下，是指执法机构、知识产权持有人，以及出于自身目的向控制人请求访问数据的其他人）的重要性？

- “正如 ICO 指南中所述，个人数据的准确性越重要，就应付出越大的努力来确保数据准确性。因此，如果您使用数据来做出可能会对相关个人或其

他人产生重大影响的决策，那么就需要投入更多的精力来确保数据准确性。”（第 14 段 - 法人与自然人）

Bird & Bird 执行摘要

本文档研究了与准确性原则相关的进一步考虑因素（有义务遵守这项原则的各方、有资格援引本原则的人员，以及评估数据准确性的基础）。其中列出了在评估数据准确性时应考虑的因素，并提供了关于提高签约方持有的注册数据准确性的措施建议。

遵守准确性原则的各方和“相关方”

控制人承担遵守 GDPR 准确性原则的义务。“准确性”和“法人与自然人”备忘录中提及的“相关方”，是指 WHOIS 数据的相关控制人。

有权援引准确性原则的各方

GDPR 规定了一系列补救措施：向监管机构投诉、司法补救措施，以及从控制人或处理人获得赔偿的权利。数据主体（以及在国家法律允许的情况下，其代表）有权采取 GDPR 规定的所有补救措施。在某些情况下，这些权利也可由其他自然人或法人行使，例如，受监管机构决定影响或因违反 GDPR 规定而遭受损害的人员。

考虑准确性时平衡各方权益

处理个人数据的目的与确定采取怎样的措施来确保数据准确性息息相关。在评估数据准确性时，必须考虑数据主体的权益。在某些情况下，控制人的利益也很重要。尽管 ICO 的准确性指南中提到几次“他人”的权利，但在我们对指南、判例法或文献的审核中，也没有进一步说明这一点。鉴于缺乏指导，我们不建议过分强调这一点。

采取合理措施确保数据准确性

文献中并未对准确性原则进行广泛的研究，而且案例法及其引用也比较有限。鉴于 GDPR 采用的基于风险的方法，应考虑确保数据准确性的措施是否合理和适当，同时还要考虑数据处理的目的和影响等因素。本文档中列出了各种建议的确保数据准确性的措施。

问题 8（自动化用例）

背景

1. 第一种情况，将在一个中央网关内执行自动化流程，负责接收来自授权用户的请求。中央网关将会自动建议是否应披露用户所请求的数据，而披露数据的最终决定将由签约方做出，签约方可以遵循或不遵循建议（场景 1.a）。对这个中央网关有足够信心的签约方可能会选择自动做出披露数据的决定（场景 1.b）。

2. 第二种情况，披露注册人数据的决定将由中央网关做出，而签约方无法审核该请求。中央网关可能会 (i) 从签约方获得相关数据并开展数据评估，然后据此做出决定（场景 2.a），或者 (ii) 在没有获得注册人数据的情况下做出决定（在这种情况下，该决定仅基于与请求者相关的信息以及在请求中做出的断言）（场景 2.b）。后一种情况的一个例子是，在针对指控商标侵权并声称代表公司处理数据，行使或辩护法律索赔的请求做出响应时，microsoft-login.com 的注册数据将自动披露给已获验证的 MICROSOFT 商标所有者。我们被要求假设每种情况都将受到一套保障措施的约束，这些保障措施作为附录 1 已被纳入本备忘录中。

A. 场景 1 下的使用案例：

根据之前在问题 1 和 2（责任）以及问题 3（自动化）备忘录中提供的建议，请为场景 1 中的每个使用案例提供以下分析：

1. 请阐述中央网关和签约方 (CP) 在以下两个问题上面临的责任风险：自动提供建议，以及就是否向第三方披露个人信息做出自动化决策。如果需要额外信息来评估风险，请记录所需的额外信息。

2. 向第三方披露个人信息的决定，是否属于第 22 条范围内所述的“对 [数据主体] 产生法律影响或类似重大影响”的决定？

3. 是否可以采取什么其他额外措施或保障措施来降低责任风险？

4. 以这种方式执行的自动化决策，是否会影响您对问题 1 和问题 2 备忘录中所述的各方的角色/责任的分析（例如，在“以自动化方式进行披露，无需任何人工的手动干预”的情况下，签约方仍然是负有责任的控制人。(1.1.4)）。

B. 场景 2 下的使用案例：

在第二种备选方案中，中央网关可根据合同，要求签约方向中央网关提供数据：

1. 备选方案会如何影响上述问题 1 至 4 中提供的分析？

2. 哪种场景对签约方的责任风险最小？对此，请说明这种假设场景下 ICANN 和签约方各自所扮演的角色，包括中央网关将决策外包给独立的法律服务提供商的情况。

C. 关于自动化的补充说明

1. 如果就是否向第三方披露个人信息做出自动化决策，那么控制人必须以何种方式向注册人阐述可能会采用自动化决策来处理其个人信息？应采用什么方式向注册人传达此类信息？以及必须向注册人传达哪些与自动化决策相关的信息，才能确保满足第 13 条规定的公平且透明的数据处理要求？

2. 控制人在上述问题 C.1 的答案中提供的信息是否会影响注册人获取以下问题的确认信息的权利：是否已就向第三方披露其个人信息做出自动化决定？是否会影响注册人获取第 15.1(h) 条中所述有意义的相关信息的权利？

3. 做出上述决定的方式，是否会影响必须提供该信息的方式？

4. 近因原则在确定数据披露决定是否会产生法律或类似重大影响时发挥着什么样的作用（即，披露注册人个人数据的决定与个人数据处理的最终法律影响或类似重大影响存在多大的关联）？如果在收到个人数据后，请求方自行处理具有法律或类似重大影响的信息，请说明这会给中央网关或签约方带来怎样的责任风险。

5. 在之前关于“自动化”的备忘录的第 1.12 节中，Bird & Bird 指出：也有可能调整 SSAD 结构，使其不会陷入“完全基于自动化处理的决策”。为了扩大范围，SSAD 可以公布其将接受的请求类别，并要求请求者确认自己提出的请求符合相关标准，而不是 SSAD 要求请求者提供信息并评估其请求是否符合发布非公开注册数据的相关标准。在这种情况下，不会出现因自动化数据处理而导致决定发布数据。出于审核目的，SSAD 可以要求请求者提供关于其请求性质的额外信息，但不会将这些信息用于评估请求本身。您能否详细说明 SSAD 如何 (i) 发布将批准的请求类别以及 (ii) 要求请求者手动选择适用的类别并确认相关请求符合相关标准，且会做出“非自动化”披露的决定？

Bird & Bird 执行摘要

本文档研究了 EPDP 团队提出的与非公开注册数据披露的自动化决策相关的场景和使用案例。本文档阐述了属于 GDPR 第 22 条范围的完全自动化决定的情况、与第 22 条相关的挑战性问题，以及可用的替代选项。本文档进一步提出了数据保护保

障措施建议，并审核了 SSAD 背景下的透明度考虑因素。最后，本文档探讨了在每种情况下各方的身份以及相关的责任风险。

符合第 22 条规定的决定和替代方案

GDPR 第 22 条适用于会产生法律影响或类似重大影响的完全自动化决定。只在有限的情况下才允许做出第 22 条中所述的决定，这些情况不太可能适用于 SSAD。只有在以下情况下，才允许做出完全自动化决定：(a) 不包括个人数据的处理；(b) 不会产生法律或类似重大影响；(c) 经适用的欧盟或成员国法律授权，其中规定了保护个人权益的适当措施；或 (d) 属于第 22 条规定的国家减损范围（例如，为了侦查刑事犯罪）。在所有其他情况下，决策过程都需要有意义的人为参与。

第 22 条规定的标准适用于 SSAD 吗？

(a) 完全自动化处理：若要适用第 22 条，需要对个人数据进行一些处理，但没有要求决定仅涉及个人数据处理。此处探讨的决定，在大多数情况下都涉及个人数据处理，无论中央网关是否能够访问所请求的数据并在决策中考虑这些数据都是如此。除了场景 1.a（即：SSAD 仅发布自动化建议）之外，所有其他场景都将包括完全基于自动化处理的决定（向第三方披露注册人数据）。

(b) 法律影响或类似的重大影响：GDPR 中没有这个术语定义；但是，其中暗示这是一个很重要的阈值。披露注册人数据是否会产生这种影响，将取决于请求的具体情况：本文档评估了每个使用案例下的数据披露影响的性质。在可能的情况下，我们给出了明确的肯定和否定答案：部分用例将受益于进一步讨论。法院或监管机构没有审核近因原则在确定某项决定的效果方面所发挥的作用。德语文献中有一些论述；然而，由于缺乏更广泛的讨论，监管机构关于这一主题的意见可能会有所帮助，因为这可能允许在中央网关/CP 仅做出一个预备性决定的基础上实现 SSAD 的自动化。

保护措施

本文档附录 2 中列出了各种建议的数据保护措施。其中包括：与监管机构合作，明确界定每个使用案例的范围并确立法律基础，向请求者施加适当的披露条款，实施适当的安全措施，采取措施遵守问责制原则，制定满足个人权益的政策，以及与处理人签订适当的数据保护条款。

透明度

提供信息的方式不受自动化决定的影响；但是，信息的内容会受到影响。

- 信息通常通过隐私声明提供；鉴于 SSAD 在域名系统中的重要性，应以突出的方式展示隐私声明。
- 由注册服务机构来提供相关信息（考虑到他们与注册人的直接关系）是最有效的，无论他们在 SSAD 环境中是否被视为控制人。如果注册服务机构不是控制人但代表控制人提供信息，则应向注册人说明情况。
- 就内容而言，仅就符合第 22 条规定的决定而言，通知还必须包括以下信息：存在自动化决定、所涉及的逻辑原因，以及数据处理的意义和预期后果。
- 需要根据请求提供 GDPR 第 15 条（访问权）的要素，即使这些内容已经包含在隐私声明中。
- 访问权要求控制人提供关于数据“已经或将被披露”的目标接收人的信息：这表明，在没有适用的豁免条款的情况下，控制方必须告知行使自身访问权的注册人其已做出向第三方披露注册人数据的决定。

相关各方的地位

(a) 在第 1 种场景下，披露注册人数据的最终决定由 CP 做出。“责任”备忘录中进行的分析在此也适用，监管机构很可能会将 CP 与 ICANN 视为联合控制人。

(b) 在第 2 种场景下，情况并不明朗。根据所采用的是宏观还是微观方法，可以发现 CP 是自动化决定和向请求者披露数据的（联合）控制人，或者仅仅只是向中央网关披露数据的控制人。我们认为第二种选项（只是向中央网关披露数据的控制人）是更好的分析，但这一点目前还不明确。将决策外包给独立的法律服务提供商不太可能会改变上述立场。

在这两种情况下，认为 CP 是处理人的论据是不合理的。

从以下方面审核了 CP 的责任：

(a) CP 的地位：如果 CP 是联合控制人，则务必在协议中明确分配各自的任务和责任。
(b) 责任类型：
- 个人的责任：规定是承担共同及连带责任，CP 可能要对由于其所涉及的处理过程造成的全部损害负责，无论其处于何种地位。他们只能通过证明他们没有以任何方式卷入造成损害的事件来避免这种情况。否则，他们有权向其他控制人索回与其责任相应的赔偿部分。
- 监管机构的责任：此处未明确规定共同及连带责任，是否应根据当事方的“责任程度”采取强制措施尚有争论的余地。

就风险而言，场景 2 似乎展现了较低的责任风险，在对个人的赔偿方面以及监管机构采取的强制措施方面都是如此。