Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

结果导向型监管
及领导和交流方面的策略和优先事项

讨论文件

2017 年 10 月 10 日

目录

十个讨论问题

“结果导向型监管”需要针对策略和优先事项，作出困难但必要的选择。数据保护机构 (DPA) 显然无法面面俱到，因此需要有策略地决定最有效的方法。

1. 数字化时代带来日益加剧的挑战和期望，尤其是在资源有限的情况下，DPA 如何（独立地或与他方合作）尽可能确保数据保护监管实践能产生最佳结果？

2. 应考虑通过哪些方法，来提高 DPA 预算以使其更切合实际？

3. 对于全球许多其他监管领域采用的方法，有何值得学习之处？

4. 能否通过阻止使用会损害隐私权的不可接受的数据，从而使人们在数字化时代能有效地享有尊严和自主权？

5. 鉴于大多数 DPA 负有众多职责，如何才能有效实现整体效能？

6. 结果导向型方法能否有效设定策略重点，以确保交流、执法和投诉处理职能相平衡？

7. 是否应将领导职能设为首要策略重点，并特别关注与受监管组织的建设性交流？

8. 哪些活动和技巧最能在实践中促进建设性交流？

9. 在全球、各地区和运作层面集合 DPA 职能的实体是否将考虑实施所提的结果导向型方法原则？

10. 如何改进所提原则？

结果导向型监管 – 领导和交流方面的策略和优先事项

介绍和总结

数据保护和隐私监管的生态系统正在快速变化，而且不仅仅限于欧盟范围内。多年来，CIPL 一直作为可信赖组织及其倡导的有效风险防范体系而受到业内的高度认可。如今，我们改为将此体系视为整体，考量如何使各个组成部分最有效地整合。

本文的具体目的是激发有关数据保护机构[1] (DPA) 如何在现代信息化社会中最大化其效能议题的讨论。

随着职能增多，期望变高，而资源却仍然有限。本文论述了是否应当以及如何采取有意识的行动，来使数据保护监管[2]更具“结果导向性”。这需要针对策略和优先事项作出困难但必要的选择。DPA 显然无法面面俱到。

CIPL 采用的结果导向型方法是指 DPA 独立地、或与他方合作来实施现代化的、有策略的监管方法，以最大化其效能，从而为个人、社会和受监管的组织实现最佳结果。具体而言，这涉及在私营和公共领域，与希望“正确行事”的组织进行响应式交流，并为其提供支持，同时对不这么做的组织进行严厉处置。

本文概括性地提出了一些原则，以用作结果导向型方法的基础。这些原则旨在支持设定策略重点，包括对不同类型的职能进行排序、选择最适当的工具，以及确定特定的目标领域、活动或组织。

结果导向型方法原则

- 数字化时代实行结果导向型监管，需要独立的数据保护机构 (DPA) 保持策略性、有效性、协调性和透明化。
- DPA 的目标是产生具有成本效益的结果，从而在实践中有效保护个人、促进负责任的数据使用，并推动繁荣发展和创新。
- DPA 应优先重视保护个人。
- 所有独立 DPA 都有责任清楚地说明其寻求的特定目标结果，以及在其监管工作中为达成该类目标结果所采用的优先事项和方法。
- 所有 DPA 的策略应尽可能地协同一致、相互补充。
- DPA 应一致地对待受监管的组织，即在领域内和跨领域采用相似方法（无论组织的类型或所处地域如何）。

[1] 本文所述的“数据保护机构”是指国际数据保护和隐私委员会议的成员。
[2]本文所述的“监管”是指“管控”或“监督”。

- 所有 DPA 都应在所有活动中采用基于风险的方法，并根据行为对个人或公众和社会价值的损害程度来确定优先事项。

- 相比于仅仅采用且过度依赖于威慑和处罚，强调领导、信息、建议、对话和支持的建设性交流方法更为有效。

- 在数据保护方面，尤其应重视信息和建议，因为这对众多组织具有广泛影响，而且相关要求并不明确，需要基于上下文背景，针对个例具体判断。

- 如果能够通过真诚对话和相互合作，来与处理个人信息的组织建立开放的建设性关系（但不能导致职责模糊），将可改善整体合规效果。

- 对于受监管的组织，尤其应基于其在合规方面展现出的诚信和尽职水平来进行评估。

- 对于希望对行为负责并“正确行事”的组织，应鼓励其证明自我，例如公开表明问责制、隐私和风险管理计划、DPO 的影响，以及如何应用标识/认证计划、BCR、CBPR 和其他问责制制度。

- 惩罚性处罚应主要针对故意、有意、严重疏忽、重复性或特别严重的不合规活动。

- 虽然处理个人投诉是保护个人的重要组成部分，但处理大量投诉不仅会造成资源紧张，还可能阻碍实现更广泛的战略性目标。应按照明确标准来严格管理投诉以确定调查程度，同时意识到投诉是宝贵的信息来源。

本文的主要目的是推动数据保护和隐私领域（包括监管机构、受监管的组织、民众、学者和专家）的讨论。

虽然本文探求提供有关应用结果导向型数据保护监管方法实践情况的洞悉，但最终仍需由 DPA 业界决定是否及如何推行此方法。如果这些原则的实质受到广泛认可，则假定可在以下四个层面采用、推广和实施修订版本：

- 在全球层面，通过国际数据保护和隐私委员会议 (ICDPPC) 来执行。[3]适当的目标日期可能是 2018 年 10 月将在布鲁塞尔举行的第 40 届国际会议。
- 在欧盟层面，通过欧洲数据保护委员会来执行。
- 在亚太层面，通过亚太隐私权机构论坛 (APPA) 来执行。
- 在操作层面，通过全球隐私权执法机构网络 (GPEN) 和 APEC 跨境隐私权执法协议 (CPEA) 来执行。[4]

[3] www.icdppc.org。
[4] CPEA (http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf) 是 APEC 成员国隐私权机构的合作执法 MOU。与其他协定一样，该协议规定，参与的机构可优先处理单项或多项执法行动。有关 CPEA，请参见第 9.2 节。

本文的结构

第 1 节详述了本文的目的和性质，并重点强调了需要通过策略性方法来设定优先事项，以取得最佳结果。此节逐一列出了对个人、DPA 和受监管者的可能益处。本文旨在为全球所有的 DPA 提供帮助，而不仅仅在于促进全球数字化经济最大化的一致性。其中特别关注欧盟地区，因为 GDPR 将会使欧盟 DPA 单独和共同工作方式发生显著变化。

第 2 节介绍了 DPA 肩负的众多职能，并特别提到了 GDPR 规定的该类职能。自 2018 年 5 月起，这将为全欧洲的 DPA 带来前所未有的关注。GDPR 列出了约 22 项单独“任务”和约 27 项单独权限，但未提及策略使命。为帮助进行动态的优先级分配，已将这些职能分为以下四类：

1. **“领导者”** – 此类职能依赖于 DPA 的专业知识、职权、支持和信息；
2. **“执法者”** – 如果侵权行为采取强制执行，尤其是对于故意或有意的违规行为；
3. **“投诉处理者”** – 如果投诉直接或间接地导致处罚或补救措施；
4. **“授权者”** – 如果需要 DPA 提供特定形式的事先授权。

第 3 节指明 DPA 面临的资源不足问题。以欧盟为例，约 2600 万家企业受欧盟 DPA 管辖。最新的可比数据表明，26 个欧盟国家/地区的平均 DPA 预算低于 0.41 欧元/人，且约为 8 欧元/企业。另一项研究表明，19 家 DPA 中只有 9 家具有 40 名以上的全职工作人员，而且其中 6 家仅有不到 30 名工作人员。该章节呼吁提高 DPA 预算，指出只需向欧盟内各受监管实体收取 20 欧元的年费，即可为欧盟 DPA 增加至少 5 亿欧元预算。

第 4 节详述了其他监管领域的有效监管实例。这些实例大多来自众多近期研究，尤其是 Christopher Hodges 教授有关《Law and Corporate Behaviour》（法律和公司行为）[5]的著作，该综合调查涵盖监管、执法、合规和道德方面的现代方法。其中重点指出，任何监管体系的最佳成效都是促进受认可的行为，并制止不可接受的行为。在实践方面，有效监管意味着确保最大化合规性。大多数组织希望通过履行自身责任来“正确行事”。这意味着，如果监管机构重视效能，必须基于与受监管者的开放建设性关系，优先执行支持职能。威慑和处罚的效果有限，应主要针对故意或有意的违法行为。

第 5 节是本文的核心章节，旨将这些经验融入隐私和数据保护监管中。其中论述了效能和结果的真正含义。该节指明，除了遵循正式要求外，监管数据保护还需在数字化时代，推动人们作为独立自主的个人富有尊严地蓬勃发展。所以，整体寻求的目标结果可表述如下：

- 否决个人享有的隐私权，防止损害其生活质量的数据使用行为；以及

[5] https://www.bloomsbury.com/in/law-and-corporate-behaviour-9781782255826/。

- 在数据使用非常普遍和流行的数字化时代，通过真正、广泛的隐私保护来推动个人生活质量改善。

该节基于职能增加和资源不足的背景，阐明需要确定策略性 DPA 优先事项，以推动实现这些结果。虽然相互之间存在较大重叠，但这四个主要类型的职能经整合后，与以下四个主要监管目标相关联：**预测 - 阻止 - 检测 - 执行**。结果导向型数据保护方法概念来自本分析，以及其他监管领域的实例。其中明确指出基于**领导**角色，尽可能与受监管实体进行对话和**建设性交流**是至关重要的优先事项。

第 6 节概述了建设性交流的实践含义，并提供了可帮助实现最佳结果的一些活动和技巧示例。应重点关注透明度、磋商、坦率交流，并利用组织遵从业界领导者以及同行和竞争压力的倾向性（“群体心理”）。

第 7 节阐明了所提结果导向型方法原则初稿，并指明可如何实施和推广这些原则（经充分讨论和修订）。

第 8 节说明了所提方法的一些潜在问题。而且，该节还说明了处理低优先级职能的后果、“监管俘获”风险，以及有关受监管者可能不愿与监管者接洽的担忧。

讨论问题

这是一篇讨论文件。因此，相关章节的末尾处提出了一些关键问题。CIPL 预期将在适当的时候，在致国际会议、Article 29 Working Party (WP29)/EDPB、APPA 论坛、GPEN 和 CPEA 领导者的公开信中提出这十个问题。为便于查看，上面第 4 页中列出了所有十个讨论问题。

声明

本讨论文件是持续动态制订的，许多所含问题尚无明确答案。很多人参与和帮助完善本文，包括现任和前任 DPA 工作人员。特别感谢国际数据保护和隐私委员会议秘书处提供其近期 DPA 统计调查的资源数据。

在 CIPL 于 2017 年 6 月在都柏林举办的研讨会上，DPA、行业和学术界人士共聚一堂，基于对此主题重要性的认可来审阅本文的草稿版本，并收集宝贵建议，尤其是阐明如何在实践中进行“建设性交流”。

CIPL 诚挚感谢自发助力此项目的各方人士。

1. 本文的目的和性质

数据保护领域至今已行至岔路口。鉴于第四次工业革命[6]和信息实践的快速演变，以及众多新颁发的数据隐私法律法规（包括欧盟 GDPR），我们面临前所未有的高风险。

所有独立的数据保护机构 (DPA) 都在落实数据保护方面扮演着重要的角色。不过有时对于 DPA 整体角色及其特定职能的认知过于理所当然，而未曾具体分析应如何在实践中履行职责。

本文旨在讨论如何在面临大量挑战和高期望的情况下，最大化监管框架的效能。具体而言，即参照许多其他监管领域的发展，推行结果导向型方法，并就此寻求各方的意见和建议。这需要实施策略性方法，来设定可实现最佳结果的优先事项。

结果导向型数据保护监管方法的全面含义和性质详述如下。不过首先，让我们先来了解本文所探讨的益处。这些益处可进行下述分类：

a. 对个人的益处

数据保护监管的基本目的必然是在促进自由数据流的同时，保护个人。[7]数据保护监管可促进信任，而这正是数字化发展和进展、数据创新以及有益数据使用所必需的。

欧盟和其他许多司法管辖区按照维护基本权利和自由表达此意。而在其他地区，则更多是为了阻止对个人的伤害。在所有情况下，都具有更广泛的“社会利益”宗旨。无论使用哪种语言，任何监管框架都应重点关注保护个人。

任何监管框架都必须是有效的，而且应主要基于对个人的影响来评估效能。是真正在保护个人，还是纸上空谈？ 个人是否获得应有的益处？ 消费者、公民、员工等个人能否在确信利益受到适当保障的情况下，充分享受数字化时代的益处？ 他们能否期望各类机构真正地正确处理其个人信息？

在与商业和公共实体打交道时，必须努力平衡个人的需求和希望。人们一般不具备相应权力、知识或能力，仅凭一己之力来保障自身利益。不过，个人的个性、态度和偏好都相差较大，因此只能假定其对自身利益具有最适当的评判。而且，市场和同行/竞争对手压力也可能对组织声誉和行为产生重大影响。任何监管实体都必须特别谨慎，以免在确定个人最佳利益时“独断专行”。现代方法优先重视对个人的保护和赋能，但不会增强或剥夺其权利。[8]

[6] 基于世界经济论坛的解释。
[7] 欧洲法院要求 DPA 在“保护私人生活权利与个人数据自由流通之间建立公平平衡”（案例 C-518/07 – 第 30 节）。
[8] EDPS 策略规定了广受欢迎的做法，即简单明确地传达艰深难懂的概念。

而且，关注个人还将帮助用平实的表述进行媒体宣传，来提升公众意识，并为数据保护活动获取民众支持。[9]只有让个人了解数据保护的重要性，并将之与自身生活相关联，才能完全实现效能。

b. 对 DPA 的益处

DPA 正面临诸多挑战。实际上，他们已变成数字化社会和社会驱动力量（即数据）的主要监管机构。他们管控数百万个组织，无论这些组织规模大小如何、是处于私营、公共还是第三部门，亦或是否跨境运营（大多如此）。创新技术的发展日新月异。个人日益明确意识到并坦率表达对隐私保护和负责任使用数据的期望。DPA 必须在诸多任务与潜在冲突的公共政策目标之间取得平衡，此类目标包括数据保护、其他基本权利（包括言论自由）、自由信息流、创新、社会利益、安全等等。

此外，在绝对意义上且相比于大多数其他监管领域，DPA 的资源一直不足。任何 DPA 都面临一项基本挑战，也就是在“人少事多”的情况下，如何才能最大化效能。虽然在个别情况下有所增加，但毫无争议的是，资源一直处于不足状态。DPA 还必须保持可信度和合法性。DPA 从来就无法面面俱到。

因此，需要改进方法，来专注于可取得最佳结果的监管活动，从而提升 DPA 的效能和影响力，并尽可能充分利用可用资源。换言之，如果 DPA 未采取积极措施来最大化效能，其可信度和合法性可能会受到影响。

鉴于跨境协作和合作要求，方法一致性需求日益加剧。应充分协调 DPA 的职责和权限，来平衡数据流全球化与在全球范围内保护个人权利的需求。在欧盟地区，GDPR 规定了此点。

对于任何此类效能期望，都需要最大限度地明确所有参与机构的策略和优先事项。结果导向型方法并不意味着标准化和通用的方法。但是，国际 DPA 业界必须至少确保互补和一致行事。虽然不同 DPA 所适用的法律体系和所处的监管文化均有所差异，但在广阔无界的数字化世界，必须保持优先事项一致，且尽可能无缝衔接。这还将促进对 DPA 资源的有效使用。

在欧盟地区，这些需求更为明显。要实现 GDPR 的协作和一致性机制，需要在优先事项、执法方法以及立法解释方面都确保一致。

国际协调计划已展现其潜在作用，例如全球隐私权执法机构网络 (GPEN) 和 APEC 跨境隐私权执法协议 (CPEA)，以及协调调查和国际互联网联合行动。

而且还增加了与消费者、竞争对手、电信公司和其他监管实体的合作。EDPS 已提出建立数字化信息交换中心，来“汇集竞争领域、消费者和数据

[9] 详述于 GDPR 第 57(1)(b) 条。

保护界的机构，以分享信息，并讨论如何最有效地基于个人利益来执行规定”。此交换中心的首次会议于 2017 年 5 月举行。[10]

c. 对受监管者的益处

无论规模大小，亦或是政府、公共机构还是 NGO，所有组织都在进行活动、产品和服务数字化；处理个人数据；并在一定程度上受数据保护法监管。基于自身性质，这些法律并非总是清楚明确的，往往视原则和具体情况而定。然而，受监管者需要了解适当行为的定义，以及应采取哪些措施来保护个人，并避免哪些举措。无论是大型组织、中小型企业还是新兴公司，所有受监管者都需要并有权同等接受国内和跨境监管机构尽可能一致和可预测的监管。这一点尤其重要，因为技术发展速度不断变快，而且现代数据保护法律日益注重问责和风险管理。

在具有顺畅自由、秩序良好的数据流的数字化经济时代，有效的监管制度对于促进创新、经济发展和繁荣必不可少。不过，该等制度不应造成不成比例的负担，尤其是成本转嫁带来的价格增长、薪资降低或税费提高。

d. 普遍适用于全球，并特别针对欧洲

虽然存在可能导致规定不适用的特定差异，但世界各地的 DPA 具有更多的共同之处。因此，本文所含的分析和建议适用于所有 DPA，将可推动最大化全球数字化经济的一致性。

与此同时，欧盟地区的 DPA 活动很快将随着 GDPR 的实行而发生显著转变。这不仅将对欧盟 DPA 造成重大影响，而且还将对其他许多 DPA 产生一定程度的直接或间接影响。重新设定 DPA 职能（尤其是一站式服务、DPA 领导者，以及具有法律约束力的协作和一致性机制）促使需要尽可能就如何最大化效能达成一致。所有欧盟 DPA 都需要重新设定策略重点，并在整个欧盟地区一致实行。鉴于本文所含的分析和建议特别针对这些挑战，CIPL 希望可借此为这些 DPA、WP29 和 EDPB（在适当的时候）提供帮助。

可以预期，此欧盟方法将在未来数年中，对全世界产生重要影响。虽然本文引用 GDPR 来详述多项要点，并预期 EDPB 可领导推行所述建议，但需要强调的是，此整体方法并不限于欧洲地区。

[10] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en。

2. 数据保护机构的职能

虽然全球各地特定 DPA 的具体职能各异，但也具有广泛的相似之处。2001 年，国际数据保护和隐私委员会议开始实施正式流程和标准，来进行数据保护机构的重新认证。[11]

DPA 的真正独立性和自主权极受重视。即便如此，DPA 仍需基于公共利益来执行任务。在 2010 年的*委员会诉德国*[12]案中，欧洲法院重点强调了 DPA 应如何根据法律规定，遵循民主社会的监察与制衡制度。

DPA 可视为“混合”实体，其职责在于确保组织履行义务，个人权利受到尊重，以及（更广泛一般的）在整个社会中保障高水平的隐私权和数据保护。此策略性目标可视为通过促进信息的自由流动和有益使用，来平衡基本权利保护，或者避免造成损害。在欧盟，欧洲法院将 DPA 的基本任务界定为“在保护私人生活权利与个人数据自由流通之间建立公平平衡”。[13]DPA 曾被称为“权威之冠”。[14]

在欧盟地区，DPA 具有宪法规定的广泛任务，来“管控”或“监督”个人数据处理，并确保遵循数据保护规定。[15]GDPR 的第 57 和 58 条列出了所有数据保护监督机构的职能，包括一些新定职能。这些职能可视为“威慑与奖励”相结合，具体可分为任务和职权两类。其中指明了约 22 项单独“任务”，这些是 DPA“应”执行的规定活动。而且详述了约 27 项职权，其中 6 项为“调查”，11 项为“纠正”，另外 10 项（包含一些上述强制性任务）为“授权和建议”。

实际上，GDPR 只是列出了这 22 项强制性任务和 27 项职权，而并未明确规定相应的优先级、指明相互之间的关联，或阐明各 DPA 在目标结果方面的整体使命。各项职能都已分别一一说明，其中大部分本身不令人意外，也不具争议性。然而批判性地来看，GDPR 未规定任何整体策略。

但 GDPR 或其他地区的法律都未禁止制定更具策略性的结果导向型方法。而且还支持识别不同**类型**的职能，这是任何策略性思考的必要元素。

虽然这些职能具有相互关联和相互依赖关系，但并无严格界限，本讨论文件的附录 A 将所有 GDPR 职能分为以下四个广泛类型：

1. ***“领导者”*** *– 此类职能依赖于 DPA 的专业知识、职权、支持和信息；*
2. ***“执法者”*** *– 此类职能针对侵权行为采取执法行动，尤其是对于故意或有意的违规行为；*

[11] https://icdppc.org/wp-content/uploads/2015/02/Criteria-and-Rules-for-Credentials-Committee-and-the-Accreditation-Principles.pdf。
[12] C-518/07 - 第 41-43 节。
[13] C-518/07 - 第 30 节。
[14] Bennett 和 Raab，《The Governance of Privacy》（治理隐私）。
[15] 《欧盟条约》第 16(2) 条和《基本权利宪章》第 8(3) 条。

3. ***“投诉处理者”*** *– 此类职能将直接或间接地基于投诉，来采取处罚或纠正行为；*
4. ***“授权者”*** *– 此类职能是指需要 DPA 提供特定形式的事先授权。*

3. DPA 资源不足

DPA 可能一直无法获得充足的可用资源，所以必须在制定策略和优先事项前，先仔细检查资源，以最大化监管效能。

a. 资源水平

为进行统计调查，ICDPPC 在 2017 年对 DPA 预算进行了最新的比较研究。[16]附录 B 中详细列出并分析了此研究所得的相关数据，并权衡了对 DPA 的一些要求。[17]

该调查收集的回复包括来自 58 个国家/地区的 87 个数据保护机构的资源数据。基于提供财务资源信息的国家/地区数据，2016 年的全球 DPA 预算总额为 887,320,351 欧元。

对于 26 个欧盟国家/地区，[18]数据表明 2016 年的预算总额为 205,703,574 欧元，而当年的总人口为 507,471,970。[19]这表明，在所有这 26 个国家/地区，人均预算低于 0.41 欧元。

对于每个DPA更具标示性的需求是将资源与受监管组织数量相挂钩的需求。欧盟统计局估算“2014 年，EU28 的商业经济体包含约 2600 万家活跃企业”。[20]假设几乎所有企业如今都在处理个人数据，也就是说 DPA 的企业平均预算仅为 8 欧元左右。

工作人员人数可进一步表明资源和能力水平。近期，有关*隐私权执法*[21]的 PHAEDRA 研究发现，2015 年欧盟地区内只有 12 家 DPA 具有超过 40 名全职工作人员，最高者具有 350 名，而最低者仅有 14 名。六家欧盟 DPA 仅有不到 30 名工作人员。

资源不足的问题由来已久，DPA 自身已对此有了充分意识。关于此问题的最新综述，可参见 2015 年 5 月欧洲数据保护机构会议上通过的决议[22]。该决议中值得关注的序言和内容摘录如下：

- “……欧洲数据保护机构现正面临诸多新挑战，这对其履行职能的方式产生影响……。”
- “……数据保护机构日益面临资金和其他资源限制，与此同时收到的要求却在增多。”

---

[16] 国际数据保护和隐私委员会议秘书处按需提供该统计调查的数据结果，网址为：https://icdppc.org/the-conference-and-executive-committee/icdppc-census/。
[17] CIPL 非常感谢 ICDPPC 提供并允许在本文中使用尚未正式发布的该调查数据。
[18] 无奥地利和克罗地亚的数据，而德国的数据低于实际值，因为 16 个联邦州中只有 7 个提供了数据。
[19] 这 26 个相关欧盟国家/地区的人口数据来自 2017 年 7 月 27 日的世界银行数据 (http://data.worldbank.org/indicator/SP.POP.TOTL)。
[20] http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics。
[21] http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf。
[22] https://edps.europa.eu/sites/edp/files/publication/15-05-20_manchester_resolution_1_en_0.pdf。

- “……书面规定的权利和义务必须始终得到执行和履行，否则就只是幻想，或者是对公民的欺骗。”
- “[会议]要求欧洲各国政府确保对数据保护机构的拨款足以使其满足日益增多的要求，并在实践工作中正式完成立法规定的要求。”

虽然 GDPR 对 DPA 规定了诸多职责，但并未增加当前极为有限的可用资金和人力资源。第 52(4) 条仅泛泛规定“所有成员国都应确保各监督机构获得必要的人力、技术和财务资源、场地和基础设施，来有效执行任务和行使权力……”。

不过，这只是一般规劝，更偏向于鼓励，而非明确或实际义务。由于规定描述并不明确，所以很难通过法律、政治或其他方式来执行。[23]欧洲委员会正在促使成员国提供充足资源，但尚未制定任何标准来评估是否充足或“必要”。

不过，已出现一些实际和潜在改善迹象。爱尔兰数据保护委员会议的预算获得了大幅增长，ICDPPC 统计调查发现单是 2015-16 年度的预算就增长了超过 20%。在荷兰，Autoriteit Persoonsgegevens (AP) 委托顾问审核其履行 GDPR 职责所需的资源。此顾问报告 [24]指出，未来的新局面将截然不同。该报告的关注重点包括：投诉和数据违规行为数量以及职责增多、欧盟合作机制导致需要进行更多系统性管控和调查、提高公众和组织意识的成本、DPIA 的事先咨询和磋商需求，以及认证和鉴定安排的相关成本。根据此情境，工作人员人数可能需要翻上三倍，从 72 人增加至最多 185-270 人。此报告目前已提交给安全和司法部，等待最终的预算决定出台。

爱尔兰、荷兰和其他地区也出现了可喜的实际或潜在预算增长迹象。然而，总体而言未发生增量级增长，情况仍然不太乐观。

最后要注意的是，目前除了大多数 DPA 应具备的法律技能外，对于 DPA 招募更多技术、沟通和其他领域专家的需求，尚无充足关注。

b. 更多资源？

毋庸置疑的是，无论欧洲 DPA 实施何种方法，都将需要更多资源。PHAEDRA 研究 [25]总结道，“如今，虽然监督机构负有职责来确保适当水平的隐私和个人数据保护，并调查和处置发生的违规行为，但面临着人力和/或预算不足的限制……。” 其中引用了欧洲联盟基本权利署 2014 年的观点：“资源问题是造成他们活动受限的最大阻碍之一”。

DPA 的可用资源远远少于竞争/反垄断机构的可用资源。Politico 近期开展的一项研究虽然不够综合详尽，但也发现“在准备实施欧盟最大隐私法方面，存在监督不足的漏

[23] 在*委员会诉奥地利*案中，CJEU 甚至未采纳 DPA 应具有单独预算的论点。
[24] https://www.tweedekamer.nl/kamerstukken/detail?id=2017D15344&did=2017D15344。

[25] 参见第 16 页。

洞”。[26]2017 年 3 月，Isabelle Falque-Pierrotin 代表 WP29 向部长理事会致信 [27]，呼吁增加资源以便 DPA“有效执行新任务、培训工作人员、升级 IT 系统、提高意识，并提供有关新规定的指导”。

GDPR 未解决 DPA 资金的潜在来源问题，而是将其交给成员国处理。此类资金主要有三个潜在来源：

- **政府资金** – 来自税收或借款的公共基金一直是大多数 DPA 的传统预算来源。但是，由于大部分政府在现今财政紧缩状况下都面临经济挑战，国家政府实际上不太可能会利用公共资金来大幅增加 DPA 的可用资源。而且，由于预算取决于政府拨款，鉴于缺少有关充足预算的宪法保障，独立性威胁始终存在。

- **罚金** – GDPR 规定违反义务的组织需要支付大额罚金。不过，如果 DPA 资金直接来源于其自身处罚违规者，将会产生扭曲的“激励”作用，所以会受到强烈反对。任何此类做法都会引起极大争议，面临道德、政治和法律质疑。

- **受监管者** – 无论是通过收费还是其他方式，监管成本都可由受监管者直接承担。“污染者付费”方法在其他监管领域愈发普遍。某些 DPA 已开始就收费服务获取收入，此类服务包括审计、培训和发行刊物。基于此方法发现增加公众对组织活动的信任和信心可为组织带来益处，并避免造成公共资金负担。而且在行政方面，非常易于操作，且成本较低。例如，GDPR 不会阻止成员国要求所有处理个人数据的组织每年直接或间接向法定 DPA 支付适量的网络费用。

  再假设几乎所有企业现今都在处理个人数据，则只需在欧盟地区向 2600 万家企业分别收取 20 欧元的象征性费用，即可获得 5.2 亿欧元的年预算总额，从而增加大量资源。如果按照组织规模越大，收费越多的标准，总额还将进一步增加。[28]

讨论问题

1. 应考虑通过哪些方法来提高 DPA 预算以使其更切合实际？

[26] http://www.politico.eu/pro/starving-watchdogs-will-police-eu-biggest-privacy-law-general-data-protection-regulation-europe/?utm_source=POLITICO.EU&utm_campaign=edc4d71000-EMAIL_CAMPAIGN_2017_04_04&utm_medium=email&utm_term=0_10959edeb5-edc4d71000-189890157。

[27] http://ec.europa.eu/newsroom/document.cfm?doc_id=43668。

[28] 在英国，注册的数据处理组织超过 400,000 个。针对大型组织的收费为 500 欧元。

4. 有效监管

目前所面临的效能挑战是利用任何可用资源来获得最佳结果。数据保护不是在真空下存在，而应多学习其他监管领域的经验。近几年已有许多有关监管效能的研究，参考文献中列举了其中一些相关研究。不过遗憾的是，这些研究大多未提及数据保护，因而可能也未受到数据保护业界重视。

在论述结果导向型数据保护监管方法的实践操作前，本节会先引用一系列重要研究发现。

a. 重要主题

虽然尚未就“最有效的做法”达成定论，而且监管界对此的态度颇为摇摆，但已确定了多个重要主题。其中包括：

- 监管实践（也就是监管者的行为）与法律法规的内容同样重要。
- 目前，以既定结果为目标（即“结果导向型”监管）被广泛认可为整体监管原则。换言之，任何有效的监管实施模式都应尽可能关注结果，不仅超越单纯的“执法”，还应抵抗住压力而不为了自身利益要求合规，或过度施以监管处罚。
- 有效监管者采用“基于风险的方法”。这意味着，监督制度（包括解释和执行）旨在管理监管目标的主要风险。[29]
- 有效监管者从多种合规工具中选择最适当的方法，来与受监管者交流，并促进对执法的“主动合规”（如果可能）。如果受监管者需要或应当负责，则此方法的相关性将更高。
- 除了自身的正式权限外，监管者还利用多种杠杆工具来确保达到标准。这些杠杆工具包括来自以下各方的影响：用户、消费者和公民（尤其是可在竞争市场和民主领域中作出选择的情况下）；受监管者的同业压力；传统媒体和社交媒体；以及政治领域。

b. 法律和公司行为

近期的一项综合研究详述了这些主题，值得认真参阅。牛津大学司法制度学教授 Christopher Hodges 在其 2015 年的著作《Law and Corporate Behaviour》（法律和

[29] 这与 GDPR 中基于风险的规定尤其相关。另请参见 CIPL 2014 年的“基于风险的隐私权方法：改善实践效能”，网址为 http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf；以及 CIPL 2016 年的“GDPR 规定的风险、高风险、风险评估和数据保护影响评估”，网址为 http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf。

公司行为）[30] 中，通过总共约 800 页的例证和分析说明，详细论述了有效监管。如书中的小标题所述，此书有关“监管、执法、合规和道德的综合理论”。[31]

Hodges 教授还基于有关人们为何遵循或违反规定，以及文化如何支持持续改进和创新的实验性证据，提出了“商业道德监管”(EBR) 概念，以通过符合社会价值观的方法来实现商业成功。[32]

最大化合规性

Hodges 认为，从本质上而言，监管与行为相关。最佳结果是促进受认可的行为，并制止不可接受的行为。在实践方面，有效监管意味着确保最大化合规性。

已有大量证据表明，现代民主国家的监管机构应如何最有效地影响商业行为，来确保最大化合规性。其中包括行为心理学结果，以及有关经济和文化激励的分析。监管本身无法确保合规，尤其是考虑到会受到客户压力、竞争对手行为、媒体评论和声誉考量的显著影响。社会规范、道德价值观和同行压力也具有重要作用。自身利益意识（将合规视为增加利润或实现其他公司目标的方法）往往是主导因素。

有效监管需要治理上述及其他相似情形，而非一味抗拒或避而不理。

现代监管方法

现代民主制度的根本基础是互相尊重，尤其是支持基本人权。通过向活跃的市场经济应用政治政策，来促使社会支持诚信企业改善公共利益。诚信企业及和谐社会基于信任，才能顺畅运作。因此，监管的重要目的是基于存在健康、可持续和不断发展的经济体，促进商界的广泛信任，进而支持就业、社会稳定和创新。无论监管对象主要是经济体还是社会体，此广泛理念都同样适用。

而且与之相应地，大部分现代监管都发展自历史模式，即强有力的个人或组织“命令并管控”下级的行为，通过实际或威胁对违规者施以严苛处罚来行使权威。即使监管实体具有强大执法权，仍必须公平相称地行事、遵循正当程序，并对自己的行为负责，此点目前已广受认可，且通常具有法律效力。

这一现代方法还要求明确了解，组织和个人为何采取特定行为，以及如何为帮助他们改进。

实验性研究发现，人们会在以下情况下遵循规定：

---

[30] 参见第 8 页。

[31] 关键要点的简短摘要可参见 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/497539/16-113-ethical-business-regulation.pdf。

[32] *道德商业监管：不断增长的实验性证据*，Christopher Hodges，牛津大学沃尔森学院。

a. 规定与其认可的价值体系相符；

b. 规定内容较为公平；且

c. 规定受到公平适用。

响应式监管

目前，大量研究结果支持“响应式”监管，即强调通过信息、建议和支持（而非威慑和处罚）进行交流。这些研究涵盖了范围广泛的大量受监管活动，包括职业健康与安全、水污染、环境保护、采矿业、食品加工、老年看护以及民用航空业。

结果，而非合规性

对于 20 世纪 90 年代突然剧增的建筑工地事故率，英国监管机构（健康与安全管理局 (HSE)）决定采用新方法，让相关方*自行负责*此问题。新方法不再逐一检查数以万计的建筑工地，而是利用在高风险领域的影响，并与能够推动广泛转变的业内相关方进行交流和建立合作关系。

此方法取得了巨大成功。从 2000-01 到 2012-13 年，致命和重大受伤事故数从 4,410 降至 2,161 (49%)。

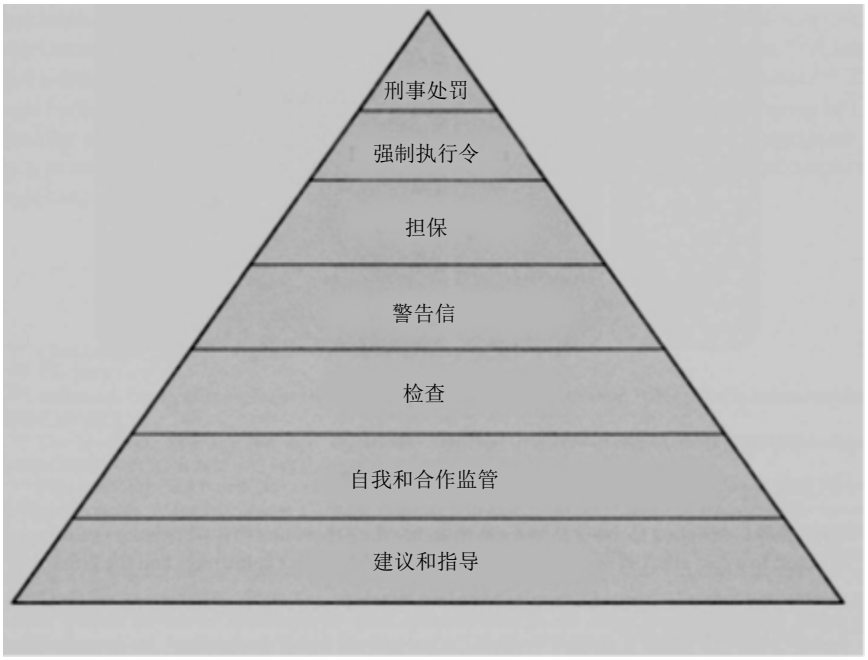
一项研究专门比较了不同国家/地区对相同法律的执法政策，并明确发现效能差异并非来自规定本身，而在于机构所采用的方法。[33]英国政府的这一做法永久降低了严重安全事故的发生率。后来，德国也实行了相同的方法，并取得同样的结果。不过，法国政府对于违规行为，仍然依赖于检查和处罚手段。这样，企业的应对诀窍是通过检查，而非确保工作场所安全。法国的工作场所安全记录在欧洲一直处于较低水平。[34]

根据这些和其他领域的经验，如果监管机构实施积极主动的方法来确保合规，将获得显著益处。这需要监管机构在执行活动时支持并帮助受监管者保持合规。特别是应优先确保提供明确的信息、指导和建议，来帮助组织履行职责。此类支持对于中小型企业更加重要，研究表明中小型企业往往在其尊重之人（例如监管机构或贸易协会）指出其尚有待改进之前，自认为遵循法律，而且在这之后中小型企业通常会接受建议并进行改进。

[33] F Blanc，《From Chasing Violations to Managing Risks. *Origins, challenges and evolutions in regulatory inspections*》（*从追查违规到管理风险：监管检查的起源、挑战和演变*）（*Edward Elgar，即将出版*）。

[34] 同上。

响应式监管 – 英国民航局的方法[35]



c. 来自其他监管领域的结论

根据所得证据和该分析，Hodges 教授总结出五个基本要点[36]：

1. **只有监管体系保持一致，并支持被广泛视为公平、相称且合乎道德的行为时，才能发挥最大效能。**
2. **各组织应负责通过证据来证明其行为可获得监管机构及其自身管理层和工作人员、客户、供应商、投资者和其他利益相关者的信任。**
3. **吸取经验教训非常重要，可通过监管机构和受监管组织之间开放的建设性交流加以促进，但会因重视归责和/或处罚而受到阻碍。**
4. **监管体系应基于以最大化合规性、繁荣发展和创新为明确目的的对话和相互合作。**
5. **如果组织违反规定，则需要采取相称的应对措施，并仅针对故意、多次或有意违规实施最严苛的处罚。**

[35]CAA 监管执法政策，基于 John Braithwaite 教授制定的“响应式”监管模式，参见《Law and Corporate Behaviour》（法律和公司行为）。
[36] 详述于附录 C。

讨论问题

1. 对于全球其他监管领域采用的方法，有何值得学习之处？

5. 结果导向型数据保护监管方法

正如前文所述，多项研究的证据和分析都一致表明，数据保护界开始兴起更具个体特异性的思维方法。DPA 和受监管组织日益意识到，合规是公司责任和可持续发展的一部分。

随着第四次工业革命推动数字化时代转型，新型数据保护生态系统正在兴起，依托于负责任的受监管组织和结果导向型的有效监管机构。

在欧盟层面，对于 DPA 根本挑战的认知逐渐增加，这些挑战可简述如下：

- 自 2018 年 5 月起，DPA 的职能将大幅扩展；
- 对于现有职能而言，DPA 资源已然不足，更不必说要履行 GDPR 规定的所有任务；
- 政府资金也无充足增长的迹象；且
- 即使是大幅增长，也不会削减对实施策略性方法的需求。

组织问责制基础是数据隐私合规的驱动因素，关于此点，CIPL 已指明多年，并在开创性的 WP29 问责制意见[37]中赋以权威认可，如今更是成为 GDPR 的核心要点。问责制也是 OECD 隐私指南中的基本要素之一。在全球范围内，加拿大、中国香港和澳大利亚隐私权委员会议的隐私管理计划指南广受认可、颇具影响力，而哥伦比亚和墨西哥数据保护法律中的问责制部分也多有引用。

2015 年，欧洲数据保护监督局 (EDPS) 在发布的意见*《实现新型数字化道德》*中指出，[38]基于 EDPS 活动，应促进与消费者和竞争法律的协同增效。[39]此 2015 年意见提出了名为“生态系统”的有效数据保护机制，所有相关方（尤其是 DPA 和管控者）更好地共同强化权利。

这位前加拿大临时隐私权委员已详细探讨了自身利益意识作为公司行为驱动因素的重要性。Chantal Bernier 的论文[40]概述了“社会许可运行”(SLO) 概念可如何促进“真正执行隐私权法律”。在该文所提的案例中，将社会接受度视为监管机构与企业之间的共同点，尤其是考虑到个人对自身期望较为“独断”，而企业则更关注处理数据声誉对本质的影响。

近期，美国商务部在 2017 年 2 月发布的一份最新报告[41]中指出，全球化经济使数据具有日益增长的普遍价值，进而产生数据保护风险和挑战，因此必须了解如何有效监管数据保护。不过，一项全球 DPA 研究表明，“具体的方法、实践和授权范围具有

[37] 有关问责制原则的 3/2010 号意见，WP 173。
[38] 4/2015 号 EDPS 意见。
[39] 例如：
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf
[40] “从社会执照到运作”概念：应用隐私权法律的共同基础？ - Dentons，渥太华。
[41] 《Seeking Solutions》（寻求解决方法），美国商务部，2017 年 2 月，
https://www.uschamber.com/sites/default/files/023052_dataprotectionhuntonpaper_fin.pdf。

较大差异”。该报告总结道，“……所有 DPA 的共同认知是，真正有效的 DPA 会将受其监管者视为合作伙伴，而非敌人”。与本 CIPL 文件所述的分析和建议相同，该报告指出了有效数据保护监管所需的七个关键属性。其中格外强调教育、意识、反馈、指导和协助。

a. 效能

对于数据保护方面的效能，尚无定论。一般而言，此效能概念经常被称为“维护个人的基本权利”、“实现高水平的数据保护”或“确保合规”。但如果没有具体目标，这些概念可能过于空洞。同样，“选择有效”等风险、优先事项、目标和口号也无实用意义，除非就“有效”的具体定义达成明确一致的共识。

一开始，所有有效监管机构都应思考：

- “我们想要取得什么结果？”
- “成功的具体标准是什么？”
- “如何确定我们很好地完成了任务？”

CIPL 对该类问题并没有答案，因为在任何情况下，都应由 DPA 自行达成协定（无论是共同还是独立地）。虽然已说明了在实践中保护个人的基本目的，但与环境保护相同，还具有更广泛的“社会公益”目的。在 CIPL 的都柏林研讨会上，针对寻求和实现明确表述的结果（不是为合规而合规）的重要性，达成了广泛共识。在该研讨会上，还认可了根本上有效的监管包括监控和改变行为及（有时）文化，而不只是确保手续和文件就绪。

因此，除了合规外，监管数据保护还意味着使人们在数字化时代富有尊严和自主权地生活。所以，整体寻求的目标结果可表述如下：

- 否决个人所享有的隐私权，防止损害其生活质量的数据使用行为；以及
- 在数据使用非常普遍和流行的数字化时代，通过真正、广泛的隐私保护来推动个人生活质量改善。

不过，必须注意，必须由 DPA 自行确定寻求取得的结果。

b. 设定战略性优先事项

任何管理有方的 DPA （通常）都需要通过公开的策略性计划，来设定明确的优先事项。即使未清晰明确地详述优先事项，实际上仍存在已完成和未完成形式的优先次序。上述会议决议已提出需要实施针对性的方法：

- “这不仅仅是资源问题。还需要数据保护机构在国家、欧盟和更广泛的欧洲层面上，实施可持续性方法来履行职能，从而针对性地完成以保护隐私为重中之重的活动……。”

但这还不够明确直白。使用熟悉的“针对”表述或采用“基于风险的方法”相对而言比较容易，而困难但正确的做法是超越修辞表达，来制定具有意义的标准、原则或其他指标，以确定应处理的优先事项、目标或风险。这至少适用于两个方面：

- 应如何对职能（或者任务或活动）进行排序？
- 应如何在特定职能中选中某一领域、活动或组织？

所有领域和司法管辖区的任何监管实体都面临这些问题。如前所述，来自其他监管领域的实例提供了答案。数据保护应吸取这些经验。特别是可利用大量现有实例证据，来指导如何设定优先事项。

以下构想可能有助于回答这些问题：

预测 - 阻止 - 检测 - 执行

对于任何监管机构，这些都是重要的目标，但必须加以权衡，并确定优先级。来自其他监管领域的实例证据表明，应以“阻止”为首要步骤，然后在必要时加以“执行”。然后，通过将这些目标与所有 DPA 职能相关联，便可制定明确策略。

结果导向型监管方法包括尽可能增加与受监管组织的交流，而且如此表所示，领导是有效实现所有目标的关键所在：

	领导者	授权者	执法者	投诉处理者
预测	✓			
阻止	✓	✓		
检测	✓		✓	✓
执行	✓		✓	✓

此分析还指明了优先事项的大致排序：

1. **“领导者”** – 重点依赖于 DPA 的专业知识、职权、影响力和信息；
2. **“执法者”** – 重点在于针对实际或潜在发生的违规行为进行执法。
3. **“投诉处理者”** – 重点在于处理个人的投诉，可能直接或间接导致采取处罚或纠正措施。
4. **“授权者”** – 需要 DPA 提供特定形式的事先授权。

c. 领导和交流

> “DPA 现今提供的指导将促成未来取得期望结果。”

此分析明确指出，指导正确实践的领导作用是首要策略重点，而且在现代信息化世界将越来越重要。这涵盖了需要实现的所有目标。

领导作用关注于依赖 DPA 专业知识和职权的职能。有效的 DPA 应当且需要发挥领导作用，来阐明预期结果和行为。这包括了解技术、商业和政治环境；预估问题；解释法律；以及提供前瞻性、实践性和策略性指导。虽然律师、顾问或其他建议者以及受监管者本身都各有角色，但不能将领导职责委派给他们。在根本上，DPA 应直接***参与***对话，并主导提供信息、建议和支持，以促进真正实现数据保护。DPA 可利用来自私营和公共领域内受监管组织的知情信息，来促进完成任务。

交流职能则需要相互信任，并加强 GDPR 的问责原则。这是一个双向过程，需要负责任的组织愿意并能够证明合规、公开说明自身活动，并分享有关一般技术和行为趋势及创新的见解。虽然领导职能主要是与受监管者进行交流，但也需要向公众提供信息、建议和提高意识。

DPA 交流职能示例

- WP29 已就未实施的草稿版“意见和指南”，进行广受认可的咨询磋商。近期示例包括领导机构、数据便携性和 DPO。
- 许多 DPA 都与相关企业讨论了人工智能 (AI) 事项，现已达成共识，“透明算法”方法的效能可能低于“AI 问责和特定检查”。
- WP29 为讨论实施 GDPR 而建立的“FabLabs”也大受好评。
- EDPS 具有系统化计划，来组织对所监督的 EU 机构的高层参观。这往往会形成协定的“自发”合规路线图，以免需要进行正式执法。[42]
- EDPS 还会定期就指南草稿，与 DPO 进行磋商。
- CNIL 的 *Pack de conformité* 计划邀请特定领域的公司共同界定该领域的 CNIL 最佳数据保护实践，从而简化了行政手续。

[42] 参见后续的 EDPS 年度报告。

- 美国 FTC 定期针对特定技术发展或前瞻性主题，举行专门研讨会和咨询会，以向重要的从业者、专家、学者和领导者征求意见和交流经验。
- DPA 也会参加 APPA 的定期半年度会议，并邀请受监管组织的代表在会上就监管机构关注的重要主题交流意见。

DPA 日益意识到与受监管组织交流和合作的益处，尤其是希望实施负责任合规方法的组织。虽然无疑存在许多“灰色地带”，但显然很少有组织会主动逃避合规。虽然许多企业（尤其是中小型企业）在此方面的认知不足，但绝大多数受监管者认可自身应履行法定义务。许多大型组织已实行详细的隐私管理计划，来提供有效的自我保证或“赢得声誉”，而不仅是单纯关注惩戒违规政策的传统“隐私权文书”做法。GDPR 也开始强调问责制和风险管理，并鼓励实行认证和标识机制，进一步支持这些趋势。至少应通过综合隐私权计划，证明已采取正式措施来实现合规。

DPA 领导职能的另一部分是促使组织实行问责制框架，并激励正确行为。这需要向能够证明持续实施问责制的组织正式提供处罚减轻制度，或者直接表明最佳实践示例，以推动市场势头和同行压力。例如，新加坡 PDPC 在 2016 年的大型国际会议和新加坡 DP 周上分发了便于参阅的手册，其中指明了新加坡超过 6 个以上组织的最佳实践，包括大型跨国公司、公共部门组织和本地创业企业。

与此同时，DPA 需要精通所用方法。例如，他们应了解风险管理的原则和逻辑，并持续改进合规政策和程序，而不是将其用于发现不足之处，组织已公开认可此点，但基于正当理由赋以低优先级。同样，DPA 有关低风险或*最低限度*活动的指导可能是基于风险方法中颇受欢迎的一部分。

d. 执法者

执法者角色（针对违规组织的调查、威胁或执法行动）非常重要，但如果真正重视广泛行为结果，则不应以此职能为首要优先事项，更不能将其视为任何 DPA 的首选方法。上面第 4 节概述的实例证据表明，这一态度不仅效率低下，而且会事与愿违，产生反作用。存在严重风险，导致受监管者形成抵御、隐匿或公开敌对态度，不太可能为本应受保护的对象带来改善成果。本就不足的资源很可能会浪费在冗长的法院抗辩上。如果以威慑恐吓为首选方法，任何监管机构都无法有效行事。

这并不是否认执法的合理角色。全球各地的 DPA 在近几年都获得了显著增强的执法权力，最显著的是 GDPR，该规范规定了高达 2000 万欧元或企业全球 4%年营业额的罚金。此类处罚可有效促使可信度、合法性和统一思想。潜在的执法和加强处罚无疑会对许多组织产生影响，尤其是在会造成商业或声誉损失的情况下。DPA 将需要在

适当考虑比例相称的前提下，不时行使执法权，以确保执法行动有意义。如果采取决定性行动，尤其是涉及严重处罚，很可能会受到关注（尤其是通过媒体和政治渠道）。

某些违规行为可能非常严重，以致于无法避免处罚。不过，执法活动的主要对象（建议指明为明确目的）无疑是参与故意、有意、多次或严重疏忽不合规的组织。此方法与 GDPR 规定相符，该规范包含多项应在确定是否处罚和罚金金额时考虑的因素。其中包括违规行为的严重程度、属于故意还是疏忽，以及任何相关的既往违规。[43]大多时候将需要发出特定形式的警告，以提醒组织，同时便于 DPA 辨别违规行为是否是故意为之。如果 DPA 要成功发挥领导职能，则应基于正当理由施以处罚，例如不合规的警告被视而不见且对个人存在实际损害的风险。

e. 投诉处理者

虽然欧盟法律将投诉机制视为个人数据保护权利的重要部分，而且投诉处理也包含在某些地区的一些数据保护法中，但在其他监管领域，很少有监管实体还具有投诉处理职能。

在欧盟地区，GDPR 强制要求 DPA“处理”投诉。不过这并不是新规定，根据现行的欧盟法律，必须通过尽职调查来处理投诉，这也是 *Schrems* 案的核心要点。[44]

但如果过度重视或未谨慎管理投诉处理职能，可能会产生严重问题和效能威胁。首先，此职能是超出 DPA 管控范围的按需实施职能，而且可能需要花费大量资源，无疑将影响其他职能的实行。除非案件经过精心挑选，否则可能会导致无法集中精力从事更具策略性的活动，而且（即使适当履行）大量投诉处理工作很少能够在领域内取得期望的行为结果。相比于关注纠正选定或多个（相对较少）个人的违规行为，监管机构应将重点放在任何不当行为发生前更普遍地保护权利。无论是造成积压还是不受认可的结果，都可能会营造公众失望或希望破灭的气氛，并危及 DPA 需要的公众支持。

当然，不应且不能完全忽略投诉处理职能。GDPR 要求 DPA 承担“处理和调查”投诉的职责。但这实际上意味着宽泛的自由裁量权。“处理”概念非常灵活，且未予以详尽解释。GDPR 的第 57(1)(f) 条要求调查应“在适当范围内”，这无疑在适当情况下允许分流安排、因投诉类型而异、基于案件严重程度来确定优先级，并将案件转介至别处。

结果导向型方法应包含以下有关投诉的部分：

- 应妥当管理投诉处理职能，以免 DPA 陷入困境；
- DPA 应留意资源使用分散和不足引起的整体效能风险；
- 应重视投诉作为情报来源的价值；
- 应将咨询和信息请求与真正的投诉相区分；

[43] GDPR，第 83(2) 条。
[44] 案例 C-362/14，Schrems，EU:C:2015:650。

- 应制定客观标准来确定可在经初始确认和监测后“调查和处理”的投诉；
- 应通过有效的分流安排，来确保公平一致地应用标准；
- DPA 应快速识别滥用、无实质价值的或无理的投诉；
- 应鼓励（或者尽可能引导）投诉者通过替代争议解决 (ADR)[45] 机制来获得救济；
- 应鼓励投诉者先向相关组织提交投诉，而该组织作为负责组织，应具有投诉处理政策和程序，并能够有效处理投诉；并
- 应鼓励实施认证和标识计划，以提供第三方争议解决安排。

所有这些举措都将减轻 DPA 处理大量投诉的负担，并使这些投诉可在源头或通过 ADR 机制获得更好的解决。而且，这将帮助 DPA 集中精力关注更严重或者未经相关组织解决的投诉。

在任何情况下，DPA 都应发布有关接收投诉的政策。借助这一方法，并遵循“适当程度”和“尽职调查”原则，可将主要精力留于处理以下投诉：

1. 累次提出影响多人的普遍违规行为；
2. 明确提出对投诉者造成严重损害；
3. 提出持续进行的严重违规行为；
4. 可通过纠正行为来大幅改进组织行为；或者
5. 提出需要实施重要的原则点。

适当方法是有效利用不足资源，并将投诉视为重要的情报来源，以补充和支持其他更重要的职能。与此同时，还指明了 DPA 不应因按需提供大量投诉解决服务而分散精力。

对上述方法的异议之一是这可能会影响个人的有效救济权利。数据保护权是个人应能够有效行使的权利。不过，CIPL 指出应更关注改善组织行为。事实上，这将普遍改善数据保护法的效能，从而强化此权利的本质（正如 CJEU 在 Costeja 案中所强调的）。[46]必须记住，与环境保护法相同，数据保护法往往被视为益于所有人的公益法律。在更具策略性的环境中，其他纠正方法也可能会发挥重要作用，来保障个人获得有效救济。

欧盟地区的尽职调查

在 *Schrems*[47] 案中，欧盟法院裁定 DPA 必须“全力执行尽职调查”来审查个人有关数据保护权的主张。虽然尽职调查的含义尚不明确，但可认为“尽职调查”要求 DPA 以适当的针对性方式来调查所有投诉。基本上，此尽职调查要求可视为 DPA 所获广泛自由裁量权与保护投诉者之间的折衷平衡。仅有有限资源的 DPA 必须确保提供高

[45] 另请参见相对较新的欧盟消费者替代争议解决 (CADR) 框架。
[46] 案例 C-131/12 *Google Spain SL*、*Google Inc. 诉 Agencia Española de Protección de Datos*、*Mario Costeja González* 案。
[47] 案例 C-362/14，Schrems，EU:C:2015:650，第 63 页。

度保护，并为在个体案例中主张发生违法行为的个人提供法定救济。由于未规定 DPA 具有义务来专门派遣资源调查所有投诉，所以尽职调查可作为折衷方法。独立 DPA 所增加的价值不仅是广泛的任务范围，更在于能够以其认为最有效的方式来执行这些任务。

f. 授权者

DPA 的授权者角色在很大程度上也属于按需职能，而且可能会花费大量资源，并且不具策略性。

在此类情况下，需要 DPA 提供特定形式的正式咨询建议、事前授权或审批。此*事前*方法意味着，如无此类授权，根本不会发生相关活动。GDPR 中列出的示例包括 BCR 审批、临时数据传输合同、无法缓解风险的 DPIA 事先磋商、行为准则等。实际授权程序不一定可在实现高行为标准方面大幅提高效能。虽然具体数量难以预测，但这可能是一项极具资源密集性的职能，尤其是如果一一处理和深入审查所有申请。

与投诉处理相同，不能忽视此职能本身及其基本原理。不过，DPA 应按照既定范围，来考量如何最有效地简化和履行此职能，尤其是在进行涉及一站式服务和一致性程序的跨境处理时。EDPB 可在此方面发挥主导作用，具体举措包括按照 GDPR 第 70(1) 条签发指南、建议和最佳实践，同时与欧盟外的 DPA 进行交流。

再次表明，需要采取策略性合作的方法。潜在富有成效的做法可能是针对既定类型的特定活动，使用给定形式的“基于类别”的审批程序，并搭配适当条件。[48]对于需要授权的所有申请，可基于针对该活动的已发布标准，轻松实施此做法。符合该标准和任何条件便可进入例行的自动授权流程，除非相关活动具有特殊或异常情况。这可与其他监管领域日益采用的“遵循或声明”方法相关联。随着 DPA 作为领导更多的与负责任的受监管者交流，对相关标准内容和适用、甚至自我认证机制存在相当大的磋商空间，DPA 或认证第三方可以进行事后审查。这显然不会取代法律明确要求的事前审批，但可大幅减轻此流程的负担。

[48] 这可能会以相似方式演变为欧盟竞争法律规定的“类别豁免”。

讨论问题

1. 数字化时代带来日益加剧的挑战和期望，尤其是在资源有限的情况下，**DPA** 如何（独立和与他方合作）尽可能确保数据保护监管实践将产生最佳结果？

2. 能否通过阻止使用会损害隐私权的不可接受的数据，从而使人们在数字化时代能有效地享有尊严和自主权？

3. 鉴于大多数 **DPA** 负有众多职责，如何才能有效实现整体效能？

4. 结果导向型方法能否有效设定策略重点，以确保交流、执法和投诉处理职能相平衡？

5. 是否应将领导职能设为首要策略重点，并特别关注与受监管组织的建设性交流？

6. 实践中的建设性交流

前一节所述的分析表明，DPA 的领导职能应作为首要的策略重点，并尽可能与受其监管者进行建设性交流。在欧盟地区，GDPR 第 57(1)(d) 条指出了此点，明确规定双方应尽可能互相协助，以实现最佳监管结果。

CIPL 于 2017 年 6 月在都柏林举办的研讨会进一步支持了此结论，该研讨会强调了监管机构与受监管者在确保实际数据隐私监管与数据创新和数字化经济发展方面的共同利益。换言之，有效的结果导向型监管机构和负责任的组织可作为现代数据保护的两个重要支柱进行更多的合作。

> “如果企业向我们证明已采取措施来确保自发合规，我们就可以放松一些，直到发现违规迹象。”
>
> “根本在于信任。监管机构和受监管者应具有相同目的。”
>
> “如果监管机构公开认可良好工作和数据保护成功实践，将产生巨大影响，并使其获得重视。”
>
> “我们已与企业合作，共同改进其行为。去年收到了来自中小型企业的 100,000 项申请。”
>
> CIPL 都柏林研讨会的参与者

该研讨会旨在探讨如何在实践中进行建设性交流。全球各地的 DPA 对建设性交流成欢迎和增多的趋势，可对此加以促进。已确定以下多项（现有和可能的）活动和技能：

- **最大化透明度** – DPA 应在设定优先事项、期望和工作方法方面保持透明化，从而帮助 DPA 提高效能，并帮助组织“一开始便正确行事”。同样，组织必须准备好透明开放地与 DPA 交流，而无需担心或受到自我控告威胁。
- **实践指导** – 基于网络的指导通常按监管要求进行解读和适用，并接受受监管组织的磋商和回应。此类指导最好采用平实的表述，并加以大量示例和分段，以尽可能便于所有目标受众应用，包括小型公司、中型企业、跨国公司、特定商业领域、公共实体等。
- **积极参与** – 在开放和封闭式会议中，为阐明忧虑和期望，参与度与发现不确定因素、趋势、商业和技术发展同等重要。
- **“受监管的自我确证”** – 完全依赖于 DPO、行为准则、认证机制、证明问责制能力等，以促进值得信任的自主合规，并减少 DPA 压力。

- **利用“无意外”方法尽可能增加磋商**，以在最终实施前获得有关指南草稿或拟议策略计划的意见或反馈。在出现新要求，或者未就“正确行事”标准或应避免的不当行为达成共识的情况下，此类对话尤为有益。
- **坦诚交流** – 愿意与市场领导者进行有关技术创新影响和接受度等方面的机密讨论。
- **利用从众心理** – DPA 日益意识到，组织倾向于遵从行业领导者。如果一或两家企业就遵从目标行动，引人注目地获得特定形式的监管背书或放行，其竞争对手、同行和许多其他方（尤其是中小型企业）也将遵从此基准，并采取相似行动。DPA 具有相当大的空间来利用此倾向，包括促进同类最佳行为；突出成功透明化、DPIA 和其他模板；展现负责任组织的最佳实践（培训或意识度宣传、DPO 领导等）；有意影响重要的法律和其他领域顾问；以及突出网络良好实践示例。
- **激励** – 如果 DPA 可为善意隐私和合规计划提供激励，公司领导层将更重视数据保护和隐私权。此类激励可能包括允许跨境分享数据、更广泛地参与大数据和机器学习活动，以及（关键地）减轻执法处罚。
- **创造负责任创新空间** – 具有相当大的空间来合作制定合规解决方案。监管沙盒（参见下文）提供了一种可能性。在数据隐私要求和合规挑战可由跨职能团队自下向上进行升级、发展时，“设计思考”提供了与其他领域中受监管组织和专家（行为经济学家、以用户为中心的设计师、技术工程师、营销和客户关系专家）进行监管参与和交流的机会。[49]
- **重复和动态合规** – 与技术和软件发展相同，如果 DPA 和受监管组织将合规视为一种历程和重复性动态过程（而非一次性活动），将会有所助益。鉴于技术发展和数字化解决方案实施速度不断加快，动态合规尤其适用于数据保护领域。这有助于基于用户反馈、内部和外部发展，以及来自行业和监管机构的经验，来促进改进。应建议组织实施动态合规方法，而且 DPA 不应对积极寻求正确行事的组织施以处罚。
- **表现指标**是必不可少的，可有效衡量和表明 DPA 是否成功地直接影响良好实践推广，建议采用通用和/或可比指标。

“监管沙盒” – 负责任创新空间

建设性交流包括为负责任的组织创造负责任创新空间。这可如何实现？

此“监管沙盒”模型由英国金融行为监管局制作 [50]，说明了如何通过有趣的方式，来支持受监管公司在受监管实体监督的“安全港”中进行试验和创新。

[49] 负责任创新举措的一个实例是 Facebook 的“设计果酱”(design jam)，该计划专门收集有关透明度和个人管控的新方法和解决方案。

[50] https://www.fca.org.uk/firms/regulatory-sandbox。

借助此监管沙盒，企业将可在实际市场面向真实的消费者，进行创新产品、服务、商业模式和交付机制测试。

此沙盒是一个“受监督空间”，可帮助组织：

- 缩短到市场的时间，并可能降低成本；以及
- 在新产品和服务中建立适当的消费者保护保障。

此沙盒提供了多种工具，例如受限授权、个别指导、豁免弃权和无强制行动函。FCA 利用针对各试点的定制监管环境，来密切监督试验。

沙盒测试应具有明确的目的（例如，降低消费者成本），并小范围执行，以便公司通过有限数量的客户，来在有限时期测试创新产品和服务。尚不能确定技术创新对数据保护的影响是否大于金融服务影响。此模型可能在数据保护界尤为适合和受认可，越来越多的业内人士意识到应将合规视为重复过程。

在此情况下潜在使用沙盒模型的做法由前 CNIL 秘书长在 2017 年初发表于《Les Echos》的文章中提出。[51]

最近（就在 2017 年 7 月），新加坡 PDPC 宣布准备与负责任的公司合作，共同制定监管沙盒，来测试拟议立法变更，并帮助这些公司保持创新力和竞争力。[52]

建设性对话必须是一个双向过程，DPA 和负责任组织应在此过程中投入充足的信任、承诺和相互尊重。除非组织能够积极帮助 DPA 对监管局面建立更佳认知，否则 DPA 不可能保持开放理解的态度。受监管企业和公共实体必须准备好且愿意与 DPA 进行建设性交流。这意味着通过尽可能开放真诚的方法，来实现积极主动、响应式的前瞻性策略。企业和政府组织需要尽可能透明公开地解释和说明其程序和技术解决方案，以及商业模式。这也属于自身利益意识，且在越来越多负责任的企业对其问责制引以为豪的环境下尤其具有前景。在制定具有明显创新性或争议性的提案时，对话对提前识别保证接受度的任何变化尤其具有价值，这比事后处理要好得多。在欧盟地区，GDPR 规定了一站式服务、DPA 领导者以及协作和一致性程序的创新机制，将可促进此双向对话，从而提高透明度，并以相互信任和尊重为基础。

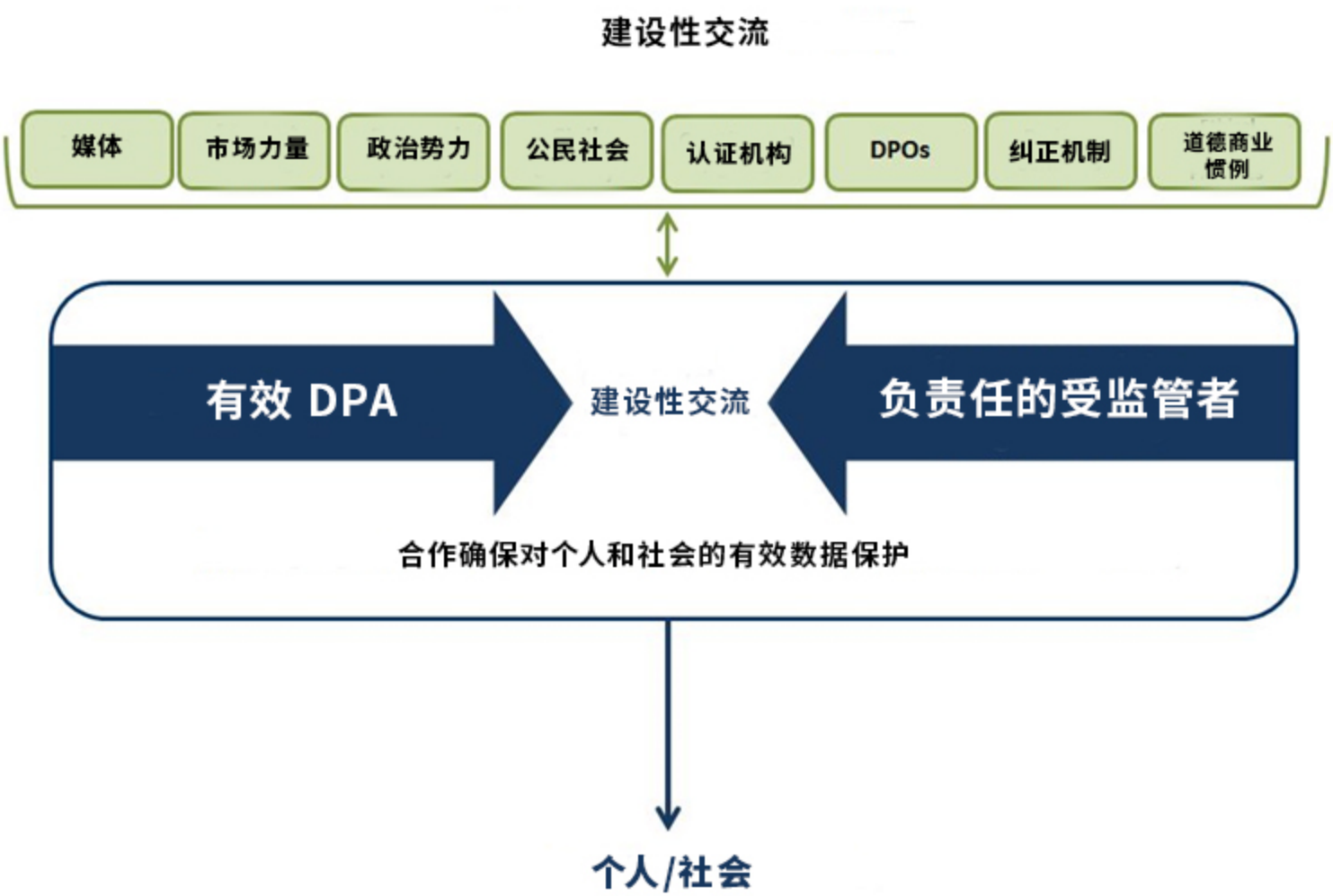
“我们需要监管机构像法官和裁判一样独立。不过，实现独立不能以损害问责制或交流为代价，而且监管机构需要通过与行业和消费者的交流，来保持市场认知…… 概括而言，监管机构必须参与但不陷入，隔离但不孤立。”[53]

[51] https://urldefense.proofpoint.com/v2/url?u=https-3A__www.lesechos.fr_idees-2Ddebats_cercle_cercle-2D165613-2Dlinnovation-2Dlautre-2Darme-2Ddu-2Dbrexit-2D2061519.php&d=DwIFAw&c=jxhwBfk-KSV6FFIot0PGng&r=Fk3CDN4QpXmXZZ7F2MuwcJTW5M0wnTw0gqFJV2no8r8&m=Yd8qNquweowj_8BlDbM5Ljgl43DBuw5ZitB6SZdhk7E&s=UHTdvy5zVo0ee3dA1N5JRiq8X9UDsOY4hU1BgUuAcUc&e。

[52] https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017。

CIPL 都柏林研讨会上也重点指出，建设性交流不能局限于直接的监管机构/受监管者关系。不仅是与数据保护受益人交流具有显而易见的重要性，而且还可借助许多其他相关方来实现目标监管结果。如前所述，可通过 DPO、第三方认证实体和纠正机制，来增强 DPA 的领导作用。利用媒体和政治力量是传播讯息的关键。在组织极其重视声誉的竞争性市场中，也需要完全了解和利用市场压力。

建设性交流是指在涵盖大量利益相关者网络贡献的“框架”中运作。下面的框架图展示了 DPA 与受监管者直接交流，以及与各类其他组织和相关方合作的范围。



讨论问题

1. 哪些活动和技巧最能在实践中促进建设性交流？

[53] “监管机构是否是新型*警察*？” Cavassini、Naru 和 Below 在《Risk & Regulation》（风险和监管）（LSE，2016 年）中提出“OECD 是独立监管机构”。

7. 结果导向型方法原则

DPA 要确保效能，必须制定策略性方法来设定优先事项和作出困难抉择。此原则适用于所有 DPA，但如同全球合作和一致性需求势必不断增加一样，还必须就如何最大限度地提高效能进行充分讨论和达成共识。

基于第 4 节所概述的有效监管一般实例，以及第 5 节中有关数据保护优先事项的具体分析，可进行综合考量，并提出待讨论的初稿，以作为结果导向型方法基础的大致原则。下述原则与某些 DPA 已采用的方法相符。此阶段所提议的原则旨在帮助确定优先级，包括设定优先事项以及选择特定领域、活动或机构两方面的内容。

此外，初步设定的原则还提供了结果导向型方法的框架，以尽可能促进 DPA 策略一致。因此，这些原则具有广泛的应用范围，适用于全球和地区层面的数据保护和隐私监管机构。上文已提及了合作确保跨境合规的重要性。但必须确保策略一致，并实现信息共享和资源集中。

如果原则内容受到广泛认可，则应可在以下四个层面实施和传播修订版本：

- 在全球层面，通过国际数据保护和隐私委员会议来执行。适当的目标日期可为计划于 2018 年秋季举行的国际会议期间。
- 在欧盟层面，通过 WP29 和（适当时）欧洲数据保护委员会来执行。理想情况下，应在 GDPR 实行日期（2018 年 5 月）之前执行。
- APPA 的亚太层面。
- 在运作层面，通过全球隐私权执法机构网络 (GPEN) 和 APEC 跨境隐私权执法协议 (CPEA) 来执行。

结果导向型方法原则

- *要在数字化时代进行结果导向型监管，需要独立的数据保护机构 (DPA) 保持策略性、有效性、协调性和透明化。*
- *DPA 的目标是取得具有成本效益的结果，从而在实践中保护个人、促进负责任的数据使用，并推动繁荣发展和创新。*
- *DPA 应优先重视保护个人。*
- *所有独立 DPA 都有责任明确开放地说明特定的目标结果，以及将在监管工作中实施的优先事项和方法。*
- *所有 DPA 的策略应尽可能地协同一致、相互补充。*
- *所有 DPA 都应在所有活动中采用基于风险的方法，并根据活动对个人或公众和社会价值的损害程度来确定优先事项。*
- *相比于过度依赖于威慑和处罚，强调领导、信息、建议、对话和支持的建设性交流方法更为有效。*
- *在数据保护方面，尤其应当重视信息和建议，因为这对众多组织具有广泛影响，而且这些要求并不明确，需要基于背景情况，针对个例具体判断。*
- *如果能够通过建设性对话和相互合作，来与处理个人信息的组织建立开放真诚的关系（但不能导致职责模糊），将可改善整体合规结果。*
- *对于受监管的组织，尤其应基于其在合规方面展现出的诚信和尽职水平来进行评估。*
- *对于希望对行为负责并“正确行事”的组织，应鼓励其证明自我，例如公开表明问责制、隐私和风险管理计划、DPO 的影响，以及如何应用标识/认证计划、BCR、CBPR 和其他问责制度。*
- *惩罚性处罚应主要针对故意、有意、严重疏忽、重复性或特别严重的违规活动。*
- *DPA 应公平一致地对待受监管的组织，即在领域内和跨领域采用相似方法（无论组织的类型或所处地域如何）。*
- *虽然处理个人投诉是保护个人的重要组成部分，但处理大量投诉不仅会造成资源紧张，还可能阻碍实现更广泛的战略性目标。投诉是宝贵的信息来源，但应谨慎管理，按照明确标准来确定调查程度。*

方案？

任何原则都是概括性和指南性的。现在考虑如何具体化这些原则并使结果导向型方法成为 DPA 的现代监管规范可能还为时尚早。而且，任何具体标准要求都可能会被视为某种形式的外部负担。

当然本文并未提出任何类型的强制要求。CIPL 明确意识到，必须由 DPA 自发努力采取结果导向型数据保护监管方法。这不仅有关独立性，只有 DPA 业界认可核心理由，此类方法才可能真正成功，绝不能强行施加。

为推进此进程以及归纳本文所提的主要想法，并推动各方进一步讨论，CIPL 特此 提出了结果导向型数据保护监管方法方案初稿。该初版方案请见本文附录 D。

与原则一样，任何 DPA 方案都仅可基于对基本框架和表述的共识，来自集体的、自发的协定和实施。为推进实施（尤其是在制定一致性机制方面），EDPB 可自行制定方案，来实施原则并推动全欧盟的 DPA 采用。

在全球范围（尤其是通过 APPA 网络和/或 GPEN 和 CPEA 的运作），DPA 可能会采用相同方案，或者在定制自己的方案之初，考虑附录 D 中的草稿方案。

讨论问题

1. 在全球、地区和运作层面集合 DPA 职能的实体是否将考虑实施结果导向型方法原则？

2. 如何改进所提原则？

8. 潜在问题

所有策略都需要作出艰难选择。应公开承认，结果导向型方法可能会带来一些挑战和风险。任何优先事项排序都必须界定先后顺序。与受监管组织进行交流可能有违常识，还会引起担忧，包括 DPA 可能会遭到“俘获”，以及某些受监管者不欢迎 DPA 过多涉入其既往、当前和未来活动。

a. 不愿意移交职能

DPA 本身会对减少任何法定职能感到紧张。如前所述，在欧盟地区，GDPR 规定的许多职能记录为 DPA“应”执行的“任务”。由于 GDPR 未为 DPA 规定任何主导的策略性目标，或者排定职能优先级的任何明确权限，因此 DPA 可能迟迟不愿进行排序。

不过，这些疑虑已有答案。虽然缺乏明确授权，但某些 DPA 已自行确定大致价值或目标。透明化的策略性方法远远胜过基于逐一事件突发的临时转变低优先级或严格管理需求并不是指完全放弃任何职能，这不是本文的意图。即使无明确的自由裁量权，仍具有评判和作出相称决定的权限。例如，其他监管实体已日益重视领导职能，认为此职能比执法职能在改变行为上更有效。事实上，任何监管机构可能采取执法行动，针对以前不视为违规的行为，施加严重处罚，这是不恰当的。

同样，完全可以实行严格管理投诉但重点关注其中部分投诉的一般政策。例如，一般接受投诉，并将其记录为问题的表面证据，但对于其中绝大多数投诉，不执行详细调查或予以解决。因此，针对各项投诉的调查深度与相关事项的潜在严重程度相对应。这需要作出严格的分类安排，以便快速评估各项投诉的关键特征，并（在大多数情况下）向投诉者告知因为资源不足，只能为其执行相称的调查。

b. 监管俘获

可能会出现过于重视与受监管者交流的担忧。如果 DPA 与受其监管组织过度接近，可能会出现“监管俘获”担忧。监管俘获是指受监管领域可能影响和操纵本应管控他们的机构。这可能构成对监管机构独立性和正直性的威胁。

毋庸置疑，监管机构必须始终适当管理与受其监管者的关系，并限制“监管俘获”风险。监管机构必须对压力保持敏感，例如此类压力可能不当影响其对监管“对象”的选择、导致过度支持受监管者需求，或者施以宽松处罚。

凭借最大限度的透明化和其他保障，对监管俘获风险的恐惧大多只在理论上。在所有领域，独立监管机构都必须能够与受其监管者建立“成熟”关系。因此，必须需要与受监管者进行接洽。有意识的开放“诚信文化”将帮助 DPA 抵抗来自受监管者的任何压力。DPA 对其独立性感到自豪，并充分意识到独立性还意味着公正，即密切关注所有问题的两面，并权衡所有事实信息。公正和正直的公司文化（可能有特定内部职能分离），将使DPA 正确决定与受监管者的适当正式和非正式交流程度。

c. 受监管者抗拒

受监管者可能也普遍担心，与监管机构过度交流将会造成问题。某些受监管组织可能希望与 DPA 保持距离，部分原因在于担心因既往的不当行为遭受处罚、因在磋商过程中向 DPA 披露文件或实践而在之后遭受执法，或者创新计划受到否决。不过，这可能会产生误导。神秘的组织可能反而会招致更多关注，而且最好提前警告违规，而不是在后期发现而花费大量成本。而且，如果 DPA 针对预计建设性关系过程中披露的信息，采取严厉执法行动，将对其自身声誉和策略造成损害风险。

如前所述，更一般地来说，交流与组织问责制密切相关，必须是基于互信的双向过程。除非受监管者也恪尽职责，否则 DPA 无法执行结果导向型方法。

附录 A – GDPR 规定的 DPA 职能

下表将 DPA 的主要任务和权限分为四个类别。本文第 5 节利用此分类来设定优先事项。

任务/权限	条款
领导者	
提高公众对风险、规定、保障和权利的意识	57(1)(b)
提高数据控制者/处理者的义务意识	57(1)(d)
为国家议会、政府等机构提供建议	57(1)(c)
向数据主体提供请求信息	57(1)(e)
监控监管适用情况	57(1)(a)
监管相关技术和商业实践等	57(1)(i)
提供有关需要 DPIA 的处理操作的建议	57(1)(l)
促进实施行为准则、认证机制，以及标识和标志体系	57(1)(m)-(q)
授权者	
基于公共利益，许可高风险处理行为	58(3)(c)
审批国际传输合同条款	58(3)(h)
审批国际传输的行政安排	58(3)(i)
审批具有约束力的公司规定	58(3)(j)
审批/认可准则、认证机制，以及标识和标志体系	42、43、57、58 和 64 *等多处*
执法者	
实施监管适用	57(1)(a)
针对监管适用情况实施调查	57(1)(h)
要求数据控制者/处理者提供信息	58(1)(a) 和 (e)
参观数据控制者/处理者所用的场地、设备和方法	58(1)(f)
签发警告和惩戒	58(2)(a)-(b)
要求合规	58(2)(c)-(e)
对数据处理施以限制和禁令	58(2)(f)
要求进行整改、消除等	58(2)(g)
施以行政处罚	58(2)(i)
暂停国际数据流	58(2)(j)
投诉处理者	
处理和调查投诉	57(1)(f)

附录 B – DPA 资源

有关 DPA 预算的最新比较调查是国际数据保护和隐私委员会议 (ICDPPC) 于 2017 年开展的研究。[54]该调查收集的回复包括来自 58 个国家/地区的 87 个数据保护机构的资源数据。基于提供财务资源信息的国家/地区数据，2016 年的全球 DPA 预算总额为 887,320,351 欧元。[55]

除了奥地利、克罗地亚和某些德国联邦州外，获得了其他所有欧洲成员国的财务资源信息。CIPL 从该调查中提取了其中 26 个欧盟国家/地区[56]的财务数据，并按照相应人口数量来进行数据比较。这些数据表明，2016 年总计 507,471,970 人的预算总额为 205,703,574 欧元。[57]这表明，在所有这 26 个国家/地区，人均预算低于 0.41 欧元。如果加入奥地利、克罗地亚和所有德国联邦州的预算值，实际数据可能会略高些。2017 年数据无疑将更高，除了葡萄牙、塞浦路斯、拉脱维亚和一个德国联邦州外，其他所有成员国的 2016 年 DPA 预算都高于 2015 年数据，但人均预算可能并未发生显著增长。

这进一步表明，所有 DPA 都需要明确确定受监管组织的数量。与大部分监管机构不同，DPA 的职责不限于特定部门，而是涵盖所有经济领域。此外，大部分公共机构也属于 DPA 的监管范围，而 GDPR 针对相应的 DPA 职责规定了一些更严格的要求。

欧盟统计局估算“2014 年，EU28 的商业经济体包含约 2600 万家活跃企业”。[58]这其中还不包括大多数公共机构。如今，很少有企业不受数据保护要求约束。即使是规模最小的一人企业也可能会在手机或笔记本电脑上，处理客户和其他联系人的个人数据。这表明在整个欧盟地区，DPA 的企业均预算为 8 欧元左右。

[54] 国际数据保护和隐私委员会议秘书处按需提供该统计调查的数据结果，网址为：https://icdppc.org/the-conference-and-executive-committee/icdppc-census/。
[55] 按照 2017 年 7 月 27 日的货币汇率，将多个国家/地区以本地币种报告的预算总额换算为了欧元金额。
[56] 德国的数据略低于实际值，因为 16 个联邦州中只有 7 个提供了数据。
[57] 人口数据来自 2017 年 7 月 27 日的世界银行数据：http://data.worldbank.org/indicator/SP.POP.TOTL。
[58] http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics。

附录 C – 来自“法律和公司行为”的基本结论

1) 只有监管体系保持一致，并支持被广泛视为公平、相称且合乎道德的行为时，才能发挥最大效能。

监管机构应采用适当的激励措施和行动，来支持（而非阻碍）个人和企业的正确行事行为。例如，监管机构应实施已发布的执法策略，来识别企业是否努力正确行事。

监管机构应警惕不能过于重视详细或法定规定（“复选框方法”），这会导致一线工作者难以自行思考，进而削减负责任行动的权限和范围。监管机构应促使成功企业实施基于价值观的文化，以推动所有人都一致关注目标结果的实现进展。例如，此类文化鼓励学习错误经验而非一味归责、在行为不当时及时调整、欢迎投诉，以及提出改进和创新想法。

2) 组织应负责通过证据，来证明其行为可获得监管机构及其自身管理层和工作人员、客户、供应商、投资者和其他利益相关者信任。

应鼓励（有时直接要求）企业在整个组织的运作中，实行负责任的业务实践。个体方面的准则尚不充足，只能实施整体方法。此方法必须从高层开始率先实施，但需延伸至组织内的各级社会团体。

监管机构应审查是否有证据可证明组织诚信运作，并实施了积极的合规方法。仅凭可靠公司自己的声称显然是不够的。有效的证据可能包括实施特定治理结构来强调合规、持续遵循行为标准、高满意客户比例、合规和审计系统的一致应用，以及透明化的外部审查方法。

3) 吸取经验教训非常重要，可通过监管机构和受监管组织之间开放的建设性交流加以促进，但会因强调归责和/或处罚而受到阻碍。

在极其重视吸取经验和保持效能的监管体系（例如民用航空、药物警戒，以及工作场所健康和安全）中，将“监管”视为行为框架，以支持人们通过不断学习来作出正确决定。

关键问题在于确定为何存在风险或问题、区分实际或潜在起因，以及如何减少相似事件的风险。重点是持续监控事件和吸取经验教训，从而改善效能并降低风险。

不过，如果人们担心会受到批评或指责，自然不愿意主动提供信息。所以在具有适当保障的情况下，必须鼓励支持分享和提问的“开放文化”，而非“归责文化”或与监管机构长期敌对。当然，对于明显或严重的不当行为，则应视为特例而进行处罚。

4) 监管体系应基于以最大化合规性、繁荣和创新为明确目的的对话和相互合作。

与管理、合规和风险体系相符的是，透明化的持续对话和合作，而非敌对和疏远的关系。所有这些都需要基于信息流通的机制，从而监控效能、识别风险并作出改进。

如果主要目的是通过最大化合规性来促进正确行为，最好将监管体系与受监督的结构化合作监管安排相结合。此类合作监管结构可包括合规和道德行为承诺，以及通过收集证据来支持信任关系的机制。

5) 如果组织违反规定，则需要采取相称的应对措施，并仅针对故意、多次或有意的不当行为，施以最严苛的处罚。

虽然无疑存在许多“灰色地带”，但现代监管机制可识别真正自发努力正确行事的组织，基本评估要点在于行事动力。必须确保采取公平相称的执法应对措施。[59]如果是故意、有意或因严重疏忽而参与违规活动，则应通过相称的应对措施来执法。但如果是努力正确行事，或者无意识地不清楚自己的职责，那么施加处罚不仅不公平，也无益于促使自愿合规。

现代执法方法基于“大部分组织大多数时候都努力正确行事”的论点。相对而言，另一种主导方法则倾向于抑制、威慑或严厉处理。通过威胁或实际施加严厉处罚来促使未来合规（或避免违规）的想法不受行为心理学（尤其是对于公司）支持。已证明，只有在视为具有造成公司或个人声誉损失（所以最好合规）的高识别风险的情况下，公司人员才会因担心违法处罚而守法。威胁对企业处以财务罚款无法有效促进合规。在现代民主社会的任何情况下，通过威胁进行监管都不会受到欢迎。

[59] 另请参见 GDPR 第 83(2) 条。

附录 D – 潜在方案初稿

结果导向型数据保护监管方法的草案

1. **数据保护机构的效能主要基于个人在实践中的受保护程度来进行评估。**

2. **数据保护机构应确保提供明确信息、指导和建议，来帮助受监管者履行既定义务。**

- DPA 应提供针对性的建议和指导，来协助受监管者了解和履行自身义务。在提供建议和指导时，应考虑这些意见的影响，以免造成不必要的负担。

- DPA 应以平实的表述记录信息、指导和建议，并针对各目标受众，采用清晰简洁、易于理解的相应格式和媒体。而且还应尽早就计划提供的指导进行磋商。

- DPA 应努力创造环境来使受监管者信任所获得的建议，并放心寻求意见，而无需担心遭受执法行动。

3. **数据保护机构还应通过简单直接的方法，来与受其监管者进行交流，以听取他们的意见。**

- DPA 应实行适当机制来与受监管者交流，使公众等各方提出观点，为有关政策和服务标准的发展作出贡献意见和建议。

- 对于违规行为，DPA 应明确界定违规事件或活动、所提供的建议、要求的行动或所作决定，以及相应理由。DPA 应提供有关建议、要求或决定的对话机会，以确保采取相称一致的行事方式。

- 如果 DPA 可证明需要采取即时执法行动来阻止或应对严重违规行为，或者提供前述机会可能有违拟定执法行动目的，则此节规定不适用。

- DPA 应确保实施了已明确解释的公平渠道，以供受监管者对其监管决定提出申诉。

- 而且，DPA 还应定期通过对受监管者进行满意度调查等方式，来征求、接收和吸取广泛反馈。

4. **数据保护机构应在开展业务中，为寻求合规的组织提供支持。**

- DPA 应基于相关因素（包括企业规模和产能，以及所处理个人数据的数量和性质），对受监管者采取相称方法。

- 在制定和审核政策、运作程序和实践时，DPA 应考虑如何支持和推动合规企业实现创新和经济发展，例如考虑如何最有效地：

- 鼓励并促进合规；
- 通过尽可能提升确定性，来提高受监管者的合规信心；
- 了解并尽可能减少监管活动造成的负面经济影响；以及
- 尽可能减少受监管者的合规成本。

5. **数据保护机构应基于风险来执行活动。**

- DPA 应采取基于证据的方法，来确定其职责领域的风险优先级，并按照能够最有效解决此类风险的方案分配资源。
- DPA 应考虑决策过程中各个阶段的风险，包括选择最适当的干预类型或与受监管者的交流方式。还应针对合规检查和执法行动选择，执行风险评估。
- DPA 应在评估风险时，检查受监管者的问责制和合规性记录（例如利用获得认可的方法），并考量有关合规的所有可用数据，包括相关外部验证证据。
- DPA 应审核所选监管活动能否有效实现目标结果，并作出任何相应的必要调整。

6. 数据保护机构应确保其监管活动方法透明一致，并与其他机构的方法充分协调。

- DPA 还应发布策略、年度工作计划、标准和目标等信息，以便受监管者作出适当预期。其中应包括以下方面的明确信息：
  - 如何与受监管者交流，以及具体的联系方式；
  - 提供信息、指导和建议的方法；
  - 检查合规性的方法，包括针对这些检查的风险评估框架详情；以及
  - 指明如何应对违规行为的执法策略。
- 在数据不受国界限制的数字化时代，DPA 应通过与其他司法管辖区的同行密切协调和合作，来最大化效能、一致性和效率。

参考文献

本讨论文件引用了多份文献的相关内容，尤其是以下出版物的帮助。

《Responsive Regulation》（响应式监管） – Ian Ayres 和 John Braithwaite，OUP，1995 年。

《A Reader on Regulation》（监管领域的读者） – Baldwin、Scott 和 Hood，OUP，1998 年。

《The Regulatory Craft》（监管技能） – Malcolm K. Sparrow，The Brookings Institution，2000 年。

《The Governance of Privacy》（治理隐私） – Colin Bennett 和 Charles Raab，MIT Press，2006 年。

《Implementing Hampton: From Enforcement to Compliance》（实施汉普顿法：从执法到合规） – UK Better Regulation Executive，2006 年。

《Really Responsive Regulation》（真正的响应式监管） – Baldwin 和 Black – LSE Working Paper，2007 年。

《Risk and Regulatory Policy - Improving the Governance of Risk》（风险和监管政策 - 改进风险治理） – OECD，2010 年。

《The Governance of Regulators - Best Practice Principles for Regulatory Policy》（治理监管机构 - 监管政策的最佳实践原则） – OECD，2014 年。

《Law and Corporate Behaviour - Integrating theories of regulation, enforcement, compliance and ethics》（法律和公司行为 - 整合监管、执法、合规和道德理论） – Christopher Hodges，Hart Publishing，2015 年。

《The European Union as Guardian of Internet Privacy》（欧盟是互联网隐私的监护者） – Hielke Hijmans，Springer，2016 年。

《Regulatory Theory - Foundations and Applications》（监管理论 - 基础和应用） – Peter Drahos，Australian National University，2017 年。