COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

《欧洲委员会条约集》第 224 号

《〈网络犯罪公约〉关于加强合作和披露电子证据的第二项附加议定书》
解释性报告

2022 年 5 月 12 日，斯特拉斯堡

---

1. 欧洲委员会部长委员会在其部长代表第 1417 次(第二期)会议(2021 年 11 月 17 日)上，通过了《〈网络犯罪公约〉关于加强合作和披露电子证据的第二项附加议定书》(“本议定书”)，本议定书于 2022 年 5 月 12 日在斯特拉斯堡开放供签署。部长委员会还注意到这份解释性报告。

2. 本解释性报告的内容旨在指导和帮助缔约国适用本议定书，并反映起草者对本议定书运作的理解。

导言

背景

3. 《网络犯罪公约》(《欧洲条约集》第 185 号，以下简称《公约》)自 2001 年 11 月 23 日在布达佩斯开放供签署以来，已成为一项对世界所有区域产生影响的文书，其成员来自世界各个区域。

4. 2003 年《〈网络犯罪公约〉关于宣告利用计算机系统犯下的种族主义或仇外行为为犯罪行为的附加议定书》(《欧洲条约集》第 189 号，下称《第一项议定书》)对《公约》作出了补充。

5. 自 2001 年《公约》开放供签署以来，信息和通信技术在全球范围内以异乎寻常的方式发展并改变了社会。然而，自那时以来，为犯罪目的利用技术的情况也显著增加。目前，许多缔约国认为，网络犯罪是对人权、法治和民主社会运作的严重威胁。网络犯罪所构成的威胁是多方面的。这方面的例子包括：对儿童的网上性暴力和其他侵犯个人尊严和人格完整的犯罪行为；盗窃和滥用个人数据，影响他人的私生活；干涉选举和对民主机构的其他攻击；对关键基础设施的攻击，如分布式拒绝服务和勒索软件攻击；或为恐怖主义目的滥用这种技术。2020 年和 2021 年，在新冠病毒大流行期间，各国观察到大量与新冠病毒有关的网络犯罪，包括攻击开发抗病毒疫苗的医院和医疗设施；滥用域名推销假疫苗、治疗和治愈方法；和其他类型的欺诈活动。

6. 尽管数据带动的技术不断发展，网络犯罪也在恶性膨胀和演变，而《公约》所体现的概念是技术中立的，因此实体刑法可适用于当前和未来的相关技术，《公约》在打击网络犯罪方面至关重要。《公约》的主要目的是：(1)统一国内实体刑法中的犯罪要件和网路犯罪领域的相关规定；(2)规定调查和起诉这类犯罪以及利用计算机系统实施的其他犯罪或与使用其他

犯罪的电子证据有关的其他犯罪所需的国内刑事诉讼法权力；(3)建立一种快速有效的国际合作机制。

7. 在适用《公约》时，缔约国尊重各国政府通过有效的刑事调查和起诉保护个人免遭犯罪之害，无论犯罪是在网上还是在网下实施的。事实上，一些《公约》缔约国认为，他们受国际义务的约束，必须提供保护手段，防止通过计算机系统实施犯罪(见 K.U.诉芬兰，欧洲人权法院(申请书第 2872/02 号，2009 年 3 月 2 日的判决/决定)提到缔约国必须根据《公约》订立的刑事调查或诉讼程序和权力)。

8. 缔约国不断努力履行打击网络犯罪的承诺，依靠根据《公约》设立的各种机制和机构，并采取必要步骤，使刑事调查和诉讼更加有效。重要的是，根据《公约》第 46 条设立的《网络犯罪公约》委员会(《公约》委员会)促进了《公约》的使用和实施。此外，欧洲委员会设在罗马尼亚布加勒斯特的打击网络犯罪方案办公室实施的能力建设方案为《公约》提供了支持，这类方案协助世界各国执行《公约》。以下三者的结合大大促进了《公约》的覆盖面和影响力：(1)《公约》在网络犯罪领域的共同标准，配合(2)缔约国通过《公约》委员会持续参与的强有力机制，以及(3)对能力建设方案的重视。

9. 2012 年，《公约》委员会根据《公约》第 46 条第 1 款规定的任务授权，交流“与网络犯罪和以电子形式收集证据有关的重大法律、政策或技术发展方面的信息”，并审议“对本公约可能的补充或修正”，设立了管辖权和跨界获取数据问题特设小组(“跨界小组”)。2014 年 12 月，《公约》委员会还完成了对《网络犯罪公约》互助条款的评估，并通过了一系列建议，包括一些将在《公约》新的议定书中处理的建议。这些努力导致在 2015 年成立了刑事司法获取云端储存的证据，包括通过法律互助获取证据工作小组(“云端证据小组”)。

10. 2016 年，云端证据小组得出结论，除其他外，“网络犯罪、设备、服务和用户(包括移动设备和服务)的数量以及随之而来的受害者数量已达到相当大的数量，以至于只有极小部分的网络犯罪或其他涉及电子证据的犯罪行为会被记录下来和加以调查。绝大多数网络犯罪受害者无法指望正义得到伸张”。该小组确定的主要挑战与“云计算、地域性和管辖权”有关，因此与有效获取电子证据或披露电子证据的困难有关。

11. 在审查云端证据小组的结论时，《公约》缔约国得出结论认为，没有必要修正《公约》，也没有必要通过实质性刑法条款规定额外的刑事定罪。然而，缔约国确定，需要采取补充措施，通过第二项附加议定书加强刑事司法机关之间的合作和获取电子证据的能力，以便能够采取更加有效的刑事司法对策以维护法治。

筹备工作

12. 《公约》委员会第 17 次全体会议(2017 年 6 月 8 日)根据《公约》委员会云端证据小组编写的提案，批准了本议定书的编写职权范围。缔约国会议决定根据《公约》第 46 条第 1 款(c)项主动着手起草本议定书。2017 年 6 月 14 日，欧洲委员会副秘书长向部长委员会(第 1289 次部长代表会议)通报了《公约》委员会的这一倡议。

13. 职权范围期最初涵盖 2017 年 9 月至 2019 年 12 月，随后由《公约》委员会延长至 2020 年 12 月，后再次延长至 2021 年 5 月。

14. 依照这一职权范围，《公约》委员会设立了一个议定书起草全体会议(起草全体会议)，由《公约》缔约国的代表以及具有《公约》委员会观察员地位的国家、组织和欧洲委员会机构的观察员组成。由《公约》缔约国专家组成的议定书起草小组(起草小组)协助起草全体会议编写议定书草案。起草小组又设立了几个分组和特设小组，就具体条款开展工作。

15. 2017 年 9 月至 2021 年 5 月期间，《公约》委员会举行了 10 次起草全体会议、16 次起草小组会议以及多次分组和特设小组会议。本议定书的大部分内容是在新冠病毒病大流行期间制定的。由于新冠疫情相关限制，2020 年 3 月至 2021 年 5 月期间，超过 65 次会议以虚拟形式举行。

16. 全体会议、起草小组以及分组和特设小组的上述工作方法，使缔约国的代表和专家能够为起草本议定书做出广泛贡献，并制订创新解决方案。

17. 欧洲联盟委员会根据欧洲联盟理事会 2019 年 6 月 6 日赋予它的谈判任务，代表属于欧洲联盟成员国的《公约》缔约国参加了这项工作。

18. 一旦条款草案编制完成并由起草全体会议临时通过，就会公布条款草案，并邀请利益攸关方提供意见。

19. 《公约》委员会与来自民间社会和私营部门的利益攸关方以及数据保护专家举行了六轮协商。这是与 2018 年 7 月在斯特拉斯堡举行的合作打击网络犯罪“八达通会议”同时举行的；2018 年 11 月在斯特拉斯堡与数据保护专家进行了磋商；2019 年 2 月邀请各方就条款草案提出书面意见；配合 2019 年 11 月在斯特拉斯堡举行的合作打击网络犯罪“八达通会议”，邀请各方于 2020 年 12 月就进一步的条款草案提出书面意见；2021 年 5 月作出书面提交和 2021 年 5 月 6 日举行了虚拟会议。

20. 此外，《公约》委员会还咨询了欧洲犯罪问题委员会(CDPC)和欧洲委员会《关于在个人数据自动处理方面保护个人的公约》的协商委员会(T-PD)。

21. 2021 年 5 月 28 日，《公约》委员会第 24 次全体会议批准了本议定书草案决定将其提交部长委员会通过。

实质性考虑

22. 就实质内容而言，本议定书工作的出发点是 2014 年《公约》委员会对《公约》互助条款的评估结果以及《公约》委员会跨界小组和云端证据小组分别于 2014 年和 2017 年提出的分析和建议。特别令人关切的是与电子证据有关的属地性和管辖权挑战，即刑事调查所需的特定数据可能存储在多个不断变化或未知的法域(“云端”)，需要有解决办法，为具体刑事调查或诉讼的目的以有效和高效的方式披露这类数据。

23. 鉴于这些挑战的复杂性，本议定书的起草者商定重点关注以下具体问题：

    在起草本议定书时，互助请求是从其他国家获取刑事犯罪电子证据的主要方法，包括《公约》的互助手段。然而，对于越来越多变化无常的电子证据请求，相互协助并非总是一种有效的处理方式。因此，人们认为有必要建立一种更为精简的机制，向其他缔约国的服务供应商发出命令或请求，要求它们提供用户信息和流量数据。

    用户信息--例如，用于识别特定电子邮件或社交媒体账户的用户或用于犯罪的特定互联网协议(IP)地址的用户--是与网络犯罪和其他涉及电子证据的犯罪有关的国内和国际刑事调查中最经常寻求的信息。缺乏这些信息，往往无法进行调查。在大多数情况下，通过互助获得用户信息并非有效，而且使互助系统负担过重。用户信息通常由服务供应商持有。虽然《公约》第 18 条已述及从服务供应商(包括其他缔约国)获取用户信息的某些方面(见《公约》委员会关于第 18 条的指导说明)，但发现有必要使用补充手段，以便直接从另一缔约国的服务供应商处获得用户信息的披露。这些工具可以提高程序的效率，也可以缓解互助系统的压力。

在刑事调查中也经常寻求流量数据，快速披露流量数据对于追踪通信来源可能是必要的，以此作为收集进一步证据或识别嫌疑人的起点。

同样，由于为犯罪目的而创建或利用的域名为许多形式的网上犯罪提供了便利，因此有必要查明注册此类域名的人。此类信息由提供域名注册服务的实体持有，即通常由注册服务商和注册管理机构持有。因此，需要一个有效的框架，以便从其他缔约国的相关实体获得这方面的信息。

在任何自然人的生命或安全面临重大和紧迫危险的紧急情况下，需要迅速采取行动，提供紧急互助或利用根据《公约》建立的每周 7 天每天 24 小时随时可用的网络联络点(第 35 条)。

此外，应更广泛地在所有缔约国之间使用行之有效的国际合作工具。根据欧洲委员会的条约(例如，《欧洲刑事事项互助公约第二附加议定书》《欧洲条约集》第 182 号)或其他双边和多边协定，已经可以采取重要措施，如视频会议或联合调查组。然而，《公约》缔约国并非普遍拥有这种机制，本议定书旨在填补这一空白。

《公约》规定了为具体的刑事调查或诉讼收集和交换信息和证据。起草者认识到，与刑事调查和起诉有关的权力和程序的确立、执行和适用，必须始终符合确保充分保护人权和基本自由的条件和保障措施。因此，有必要列入一个类似于《公约》第 15 条的关于条件和保障措施的条款。此外，由于认识到许多缔约国要求保护隐私和个人数据，以履行其宪法和国际义务，起草者决定在本议定书中规定具体的数据保护保障措施。这种数据保护保障措施是对《公约》许多缔约国义务的补充，这些缔约国也是《关于在自动处理个人数据方面保护个人的公约》(《欧洲条约集》第 108 号)的缔约国。在 2018 年 10 月起草本议定书期间，该公约的修正议定书(《欧洲委员会条约集》第 223 号)已开放供签署。还应当指出，本议定书的起草过程包括当时不受欧洲委员会数据保护文书或欧洲联盟数据保护规则约束的缔约国。因此，做出了重大努力，以确保本议定书平衡地反映可能成为其缔约国的国家的许多法律制度，同时尊重按照《公约》其他缔约国的宪法和国际义务的要求确保保护隐私和个人数据的重要性。

24. 起草者还审议了其他措施，经充分讨论后未在本议定书中保留这些措施。其中两项条款，即“利用计算机系统进行秘密调查”和“扩大搜查范围”，引起了缔约国的高度兴趣，但发现需要额外的工作、时间和与利害关系方的协商，因此认为在拟订本议定书所规定的时间范围内不可行。起草者建议，以不同的形式并可能在一项单独的法律文书中探讨这些问题。

25. 总的来说，起草者认为，本议定书的规定无论从操作角度还是从政策角度来看都将增加了诸多价值。本议定书将大大提高缔约国的能力，加强缔约国之间以及缔约国与服务供应商和其他实体之间的合作，并为具体刑事调查或诉讼的目的获得电子证据的披露。因此，本议定书与《公约》一样，旨在提高执法机关打击网络犯罪和其他犯罪的能力，同时充分尊重人权和基本自由，并强调建立在信息自由流动基础上的互联网的重要性和价值。

本议定书

26. 如序言所述，本议定书旨在通过与主管机构之间更有效的互助和其他形式的合作有关的额外手段，进一步加强打击网络犯罪方面的合作，以及刑事司法机关为具体的刑事调查或诉讼程序收集电子形式的刑事犯罪证据的能力；紧急情况下的合作(即任何自然人的生命或安全面临重大、迫在眉睫的危险的情况)；以及主管机构与服务供应商和拥有或掌控有关信息的其他实体之间的直接合作。因此，本议定书的目的是对《公约》作出补充，并在《公约》缔约国之间对《第一项议定书》作出补充。

27. 本议定书分为四章：一、共同条款；二、加强合作的措施；三、条件和保障；四、最后条款。

28. 第一章的共同条款涵盖本议定书的目的和范围。与《公约》一样，本议定书涉及具体的刑事调查或诉讼程序，不仅涉及网络犯罪，还涉及任何牵扯到电子形式证据的刑事犯罪，通常被称为“电子证据”或“数字证据”。本章还规定了适用于本议定书的《公约》定义，并载有本议定书中经常使用的术语的补充定义。此外，考虑到对相互协助和其他形式合作的语言要求往往妨碍程序的效率，增加了一条关于“语言”的条款，以便在这方面采取更务实的做法。

29. 第二章载有本议定书的主要实质性条款，其中说明了缔约国可采用的各种合作方法。不同的原则适用于各种类型的合作。因此，有必要将本章分为几节：(1)第二章适用的一般原则；(2)加强与其他缔约国供应商和实体直接合作的程序；(3)加强官方机构之间就披露存储的计算机数据开展国际合作的程序；(4)关于紧急互助的程序；(5)在无适用的国际协议情况下有关国际合作的程序。

30. 第三章规定了条件和保障。它们要求缔约国对本议定书的权力和程序也应适用与《公约》第 15 条类似的条件和保障。此外，本章还包括一套详细的个人数据保护措施。

31. 第四章最后条款中的大多数与欧洲委员会条约的标准最后条款相似，或者规定《公约》条款适用于本议定书。但是，第 15 条“本议定书的效力”、第 17 条“联邦条款”和第 23 条“缔约国协商和执行情况评估”在不同程度上与《公约》的类似条款有所不同。最后一条不仅使《公约》第 46 条也适用，而且还规定缔约国应定期评估本议定书各项规定的有效利用和执行情况。

对本议定书条款的评注

第一章　共同条款

第 1 条　目的

32. 本议定书的目的是补充：(a)本议定书缔约国之间的《公约》；和(b)同为《第一项议定书》缔约国的本议定书缔约国之间的《第一项议定书》。

第 2 条　适用范围

33. 本议定书的一般适用范围与《公约》相同：本议定书的措施在本议定书缔约国之间适用于与计算机系统和数据有关的刑事犯罪的具体刑事调查或诉讼(即《公约》第 14 条第 2 款(a)项和(b)项所述的犯罪)，以及以电子形式收集刑事犯罪的证据(《公约》第 14 条第 2 款(c)项)。正如《公约》解释性报告第 141 段和 243 段所解释的那样，这意味着，无论是使用计算机系统实施的犯罪，还是没有利用计算机系统实施的犯罪(例如谋杀)但涉及电子证据，都可以利用本议定书规定的权力、程序和合作措施。

34. 第 1 款(b)规定，在同属本议定书缔约国的《第一项议定书》缔约国之间，用于根据《第一项议定书》确立的有关刑事犯罪的具体刑事调查或诉讼程序。非《第一项议定书》缔约国的本议定书缔约国不承担对这些罪行适用本议定书条款的义务。

35. 根据第 2 款，如果缔约国的条约、法律或安排尚未包含此类规定，则需要有法律依据来履行本议定书中规定的义务。这并没有将明确的自由裁量条款变为强制性条款，有些条款允许作出声明或保留。一些缔约国可能不需要任何执行立法就能适用本议定书的规定。

第 3 条　定义

36. 第 1 款将公约第 1 条(“计算机系统”、“计算机数据”、“服务供应商”和“流量数据”)和第 18 条第 3 款(“用户信息”)中规定的定义纳入了本议定书。起草者列入了《公约》中的这些定义，是因为本议定书的执行部分和解释性报告中使用了这些术语。起草者还打算将《公约》解释性报告和指导说明(由《公约》委员会通过)中与这些术语有关的解释同样适用于本议定书。

37. 《公约》案文中所列罪行和其他术语的定义旨在适用于本议定书缔约国之间的合作，而《第一项议定书》条文中所列的罪行和其他术语的定义旨在适用于《第一项议定书》缔约国之间的合作。例如，第 2 条第 1 款规定，“本议定书所述措施应适用于……本议定书的《公约》缔约国之间与计算机系统和数据有关的刑事犯罪的具体刑事调查或诉讼”。因此，在根据本议定书就与儿童色情有关的犯罪进行合作时，适用《公约》第 9 条第 2 款中“儿童色情制品”的定义，并适用《公约》第 9 条第 3 款中“未成年人”的定义。同样，在加入本议定书的《第一项议定书》缔约国之间，《第一项议定书》第 2 条中关于“种族主义和仇外材料”的定义也适用。非《第一项议定书》缔约国的本议定书缔约国不承担适用《第一项议定书》中规定的术语或定义的义务。

38. 第 3 条第 2 款包括适用于本议定书和本议定书下的合作的补充定义。第 2 款(a)项将“中央机关”定义为“有关缔约国根据现行统一或对等立法为基础的互助条约或安排指定的一个或多个中央机关，如果没有，则指一缔约国根据《公约》第 27 条第 2 款(a)项指定的一个或多个中央机关”。本议定书在若干条款中使用了中央机关，以便通过缔约国已经使用和熟悉的渠道提供合作。因此，在统一或对等立法基础上订有互助条约或安排的缔约国必须利用根据这些条约或安排指定的中央机关。如果有关缔约国之间未订立此类条约或安排，则这些缔约国应使用其目前根据《公约》第 27 条第 2 款(a)项使用的同一中央机关渠道。虽然并非所有以统一或对等立法为基础的互助条约或安排都将使用“中央机关”这一术语，但起草者打算用这一术语来指此类条约或安排中指定的协调机关，无论其中的名称如何。

39. 除非本议定书另有具体规定，缔约国为本议定书之的目的使用此种中央机关渠道，并不意味着适用此类互助条约或安排的其他规定。

40. 第 2 款(b)项中“主管机构”的定义仿照了《公约》解释性报告第 138 段。由于这一术语在本议定书中经常使用，为便于参考，故将其定义放在执行部分的案文中。

41. 第 2 款(c)项将“紧急情况”定义为“任何自然人的生命或安全面临重大、迫在眉睫的危险的情况”。第 9、10 和 12 条使用了这一术语。本议定书中“紧急情况”的定义旨在规定一个比《公约》第 25 条第 3 款中“紧急情况”高得多的门槛。起草这一定义也是为了让缔约国考虑到本议定书中使用这一术语的不同情况，同时考虑到缔约国的适用法律和政策。

42. 紧急情况的定义涵盖重大和迫在眉睫的危险，这意味着它不包括对人的生命或安全的危险已经过去或并不重大的情况，或可能存在并非迫在眉睫的未来风险的情况。提出这些重要性和紧迫性要求的原因在于，第 9 条和第 10 条规定，被请求方和请求方都有义务在紧急情况下以更快的速度作出反应，这就要求对紧急请求给予比其他重要但不太紧急的情况以更高的优先地位，即使这些请求是在较早的时候提出的。“任何自然人的生命或安全面临重大、迫在眉睫的危险”情况，可能涉及，例如，人质情况，在这种情况下，有可信的危险，即将对受害者造成生命损失、严重伤害或其他类似的伤害；正在进行的对儿童的性虐待；恐怖主义袭击

发生后随即发生的情况，当局设法确定袭击者与谁联系，以判定是否即将发生进一步的袭击；以及对关键基础设施安全的威胁，其中对任何自然人的生命或安全面临重大、迫在眉睫的危险。

43. 正如本议定书第 10 条第 4 款和本解释性报告第 154 段(涉及第 9 条)所解释的那样，被请求方将根据这些条款确定是否存在“紧急情况”，适用本条的定义。

44. 第 2 款(d)将“个人数据”定义为“与已辨识或可辨识的自然人相关的信息”。“可辨识的自然人”是指可直接或间接识别的人，特别是可通过身份证号码或一个或多个与其身体、生理、心理、经济、文化或社会特征有关的因素来识别的人。本议定书中“个人数据”的定义与其他国际文书中的定义相一致，例如经附加议定书修订的《关于在自动处理个人数据方面保护个人的公约》、2013 年经济合作与发展组织(经合组织)《关于个人数据隐私保护和跨境流动的准则》、欧盟《通用数据保护条例》和《数据保护执法指令》、以及《非洲联盟网络安全和个人数据保护公约》(《马拉博公约》)。

45. 如果辨识需要超出合理范围的时间、精力或资源，则视此人为不“可辨识”。虽然某些信息可能是某一特定个人所独有的，因此本身就能与该人建立联系，但其他信息只有在与其他个人或识别信息相结合时才能进行识别。因此，如果根据与这些额外信息的联系来识别一个人需要超出合理范围的时间、精力或资源，有争议的信息即不构成个人数据。一个自然人是否能够被辨识或可以直接或间接被辨识，取决于具体环境(并可能随着技术或其他发展而改变)。

46. 本议定书规定的数据保护要求不适用于不属于“个人数据”的数据，例如，在合理的时间、精力或资源的情况下无法重新识别的匿名信息。

第 4 条　语言

47. 第 4 条规定了根据本议定书向缔约国和服务供应商或其他实体致函时可使用的语言范围。即使缔约国在实践中能够使用其官方语言以外的语言工作，这种可能性也可能是国内法或条约所没有预见到的。本条的目的是在本议定书下提供更多的灵活性。

48. 与电子证据有关的互助请求翻译不准确或费用高是一个急需要关注的长期抱怨问题。这一障碍削弱了获取数据和保护公共安全的合法程序。同样的考虑也适用于传统互助以外的情况，例如，一缔约国根据第 7 条直接向另一缔约国境内的服务供应商传送命令，或根据第 8 条请求执行命令。虽然机器翻译能力有望得到改善，但目前还不够。由于这些原因，在关于拟列入本议定书的条款的提案中反复提到了翻译问题。

49. 非常见语言之间的翻译是一个特殊的问题，因为这种翻译可能会大大延迟请求，或者实际上无法满足请求。翻译也可能包含严重的误导，因质量差而浪费双方的时间。然而，在使用非常见语言的情况下，请求方过多地承担翻译费用和困难。

50. 由于这种过分的负担，一些非英语国家缔约国要求在本议定书中规定使用英语。它们指出，英语是主要服务供应商普遍使用的语言。此外，随着数据在世界范围内的流动和存储越来越广泛，越来越多的国家参与到相互协助中，翻译可能会变得更加繁重和不切实际。例如，两个缔约国可能使用不太常见的语言，地理上相距遥远，而且很少接触。如果甲方突然需要乙方的帮助，可能找不到翻译乙方语言的翻译，或者最终的翻译可能比非母语英语更难理解。起草者特别强调，为加快协助速度，应尽一切努力接受特别是根据本议定书提出的英语或共用语言的紧急请求，而不是要求翻译成被请求方的官方语言。

51. 本议定书的起草者最后认为，本议定书不应强制规定使用英语。一些缔约国的官方语言要求排除了这种授权；许多缔约国使用同一种语言，因此不需要使用英语；在一些缔约国，首都以外的官员不太可能读懂英语，但往往参与执行请求。

52. 因此，第 1 款的措词是“被请求方或根据第 7 条第 5 款通知的缔约国所能接受的语言”。该缔约国可具体规定可接受的语言——例如英语、西班牙语或法语等广泛使用的语言——即使其国内法或条约中未作规定。

53. 第 1 款中使用的“请求、命令和所附资料”指的是：

第 8 条下的请求(第 3 款)、命令(第 3 款(a)项)、证明资料(第 3 款(b)项)和特殊的程序性指示(第 3 款(c)项)；

对于根据第 7 条第 5 款要求发出通知的缔约国，命令(第 3 款)、补充资料(第 4 款)和事实摘要(第 5 款(a)项)；

根据第 9 条提出的请求(第 3 款)。

“请求”还指根据第 10 条、第 11 条和第 12 条提出的请求的内容，其中包括作为请求一部分的文件。

54. 在实践中，某些国家可能准备接受以国内法或条约中规定的语言以外的语言提出的请求和命令。因此，《公约》委员会每年一次，将对请求和命令的可接受语言进行非正式普查。缔约国可以在任何时候变更该信息，任何此类变更将通知所有缔约国。缔约国可以声明只接受特定语言的某些形式的协助。这项普查结果将向《公约》所有缔约国公布，而不仅仅是本议定书的缔约国。

55. 这项务实的规定显示出加快合作的极端重要性。它为缔约国为本议定书的目的接受更多的语言提供了条约依据。

56. 在许多情况下，缔约国签订了互助条约，规定了根据这些条约提出的请求必须使用的一种或多种语言。本条不干涉缔约国之间的这些条约或其他协议的条款。此外，预计就本议定书而言，“被请求方或根据第 7 条第 5 款通知的缔约国所能接受的语言”将包括这些条约或协议所规定的任何一种或多种语言。因此，请求方应将互助条约或其他协议中规定的语言适用于根据本议定书提出的请求和通知，除非被请求方或被通知方表示也准备接受其他语言的这种请求或通知。

57. 一缔约国愿意接受其他语言，将由它向《公约》委员会表明，即它打算接受依据本议定书以另一种语言提出的部分或所有类型的请求或命令通知。

58. 第 2 款确定了根据第 7 条和第 6 条发文方应使用何种语言分别向在另一缔约国境内提供域名注册服务的服务商或实体发出命令或提出请求及附带信息。这一规定旨在确保迅速合作和提高确定性，而不会在服务供应商或实体收到披露数据的命令或请求时带来额外负担。第 2 款(a)项规定的第一种选择表明，命令或请求可以用服务供应商或实体通常接受本国当局在具体刑事调查或诉讼范围内发出的国内命令或请求的语言提交(“比照国内程序”)。对于拥有一种或多种官方语言的缔约国，这包括其语言之一。第 2 款(b)项中提供的第二种备选方法表明，如果服务供应商或实体同意接受另一种语言的命令或请求，例如其总部使用的语言，则可以用该语言提交此类命令和附带信息。作为第三种备选方法，第 2 款(c)项规定，如果命令或请求及附带信息不是以前两种选择中的一种语言发出的，则应随附上述语言之一的译文。

59. 第2款中使用的“根据第7条发出的命令和根据第6条提出的请求以及任何附带信息”是指：

第 6 条下的请求(第 3 款)；和

第 7 条下的命令(第 3 款)和补充信息(第 4 款)。

60. 如果一缔约国根据第 7 条要求通知，请求方必须准备以要求通知的缔约国所接受的语言传送命令和任何附带信息，即便服务供应商接受其他语言。

61. 《公约》委员会还将非正式力争收集有关根据第 4 条第 2 款向服务供应商和提供域名注册服务的实体发出命令和请求及附带信息的语言方面的信息，并作为上述解释性报告第 54 段所述普查的一部分，并让缔约国了解这些信息。

第二章 加强合作的措施

第 1 节 第二章适用的一般原则

第 5 条 第二章适用的一般原则

62. 第 5 条第 1 款明确规定，如同《公约》第 23 条和第 25 条第 1 款一样，缔约国应按照第二章的规定“最大限度地”予以合作。这一原则要求缔约国提供广泛的合作，尽量减少妨碍信息和证据在国际上顺利迅速流通的障碍。

63. 第 2 至 5 款将本议定书的七项合作措施分为四个不同部分，紧随第一部分的一般原则之后。这些部分按寻求合作的类型划分：第 2 节涉及与私营实体的直接合作；第 3 节载有官方机构之间为披露所储存数据加强国际合作的形式；第 4 节规定了紧急情况下的互助；最后第 5 节规定了在没有条约或安排的情况下根据有关缔约国之间的统一或对等立法适用的国际合作条款。这些章节的编排也大致因循以下递进步骤：从调查初期经常寻求的调查协助形式——获得域名注册和用户信息的披露，到请求提供流量数据，然后是内容数据，随后是视频会议和联合调查小组，后者是在调查后期经常寻求的协助形式。

64. 关于一般原则一节，它明确了每项措施在何种程度上受到或不受有关缔约国之间在统一或对等立法基础上的互助条约或安排的影响，即请求方和被请求方进行政府间合作，以及寻求信息的缔约国和拥有或掌握这种信息的私人实体所在的缔约国根据第 6 条和第 7 条进行直接合作。“以统一或对等立法为基础的安排”是指“例如北欧国家之间建立的合作制度，该制度也得到《欧洲刑事事项互助公约》(第 25 条第 4 款)以及英联邦成员国之间的承认”(见《公约》解释性报告第 263 段)。本章第 2 至 4 节中的措施适用于所涉缔约国，无论它们是否在统一或对等立法的基础上相互受到适用的互助协议或安排的约束。除非另有规定，第 5 节中的国际合作条款仅在没有此类协议或安排的情况下适用。

65. 如本条第 2 款所述，本章第 2 节由题为“有关域名注册信息的请求”的第 6 条和题为“披露用户信息”的第 7 条组成。这些条款即所谓的“直接合作”条款，允许缔约国的主管机构为具体刑事调查或诉讼的目的，直接与私营实体——即第 6 条中提供域名注册服务的实体和第 7 条所述的服务供应商——进行接触。无论寻求信息的缔约国与拥有或掌握此类信息的私营实体所在的缔约国之间是否存在基于统一或对等立法的互助条约或安排，第 2 节均适用。

66. 如本条第 3 款所述，本章第 3 节由题为“执行另一方关于加快提供用户信息和流量数据的命令”的第 8 条和题为“紧急情况下快速披露存储的计算机数据”的第 9 条组成。这些措施是

“加强官方机构之间的国际合作”，即规定主管机构之间进行合作，但性质与传统的国际合作不同。无论请求方和被请求方之间是否有一项以统一或对等立法为基础的有效互助条约或安排，第 3 节均适用。

67. 如本条第 4 款所述，本章第 4 节由题为“紧急互助”的第 10 条组成。虽然紧急互助是一项互助条款，但它是应对紧急情况的一项重要合作工具，许多互助条约都没有对此作出明确规定。因此，起草者决定，无论有关缔约国之间是否根据现行的统一或对等立法订立了适用的互助协议或安排，本节均应适用。关于规范紧急互助的程序，有两种可能性。当有关缔约国在统一或对等立法的基础上相互受适用的互助协议或安排的约束时，第 4 节由该协议的规定加以补充，除非有关缔约国共同决定适用《公约》的某些规定来代替该协议(见本议定书第 10 条第 8 款)。如果有关缔约国相互不受这种协议或安排的约束，则缔约国适用《公约》第 27 条和第 28 条规定的关于在无条约情况下相互协助的某些程序(见本议定书第 10 条第 7 款)。

68. 如本条第 5 款所述，本章第 5 节由题为“视频会议”的第 11 条和题为“联合调查组和联合调查”的第 12 条组成。这些规定是国际合作措施，只有在请求方和被请求方之间没有根据现有统一或对等立法订立的互助条约或安排的情况下才适用。这些措施不适用于存在这种条约或安排的情况，但不论是否存在这种条约或安排，第 12 条第 7 款均适用。但是，有关缔约国可相互决定适用第 5 节的规定，以代替现有的条约或安排，除非条约或安排的规定禁止这样做。

69. 第 6 款仿照《公约》第 25 条第 5 款，因此《公约》解释性报告第 259 段在此也适用：“如果允许被请求方要求双重犯罪作为提供协助的条件.....如果被请求协助所涉及的行为也是被请求方法律规定的刑事犯罪，即便被请求方的法律将该罪行归入不同的犯罪类别或使用不同的术语命名该罪行，则应视为存在双重犯罪。为确保被请求方在适用双重犯罪时不会采用过于僵硬的检验标准，这一规定被认为是必要的。鉴于各国法律制度的不同，犯罪行为的术语和分类必然会出现差异。如果这种行为在两种制度下都构成犯罪，这种技术差异不应妨碍协助。相反，在适用双重犯罪标准的事项上，应以灵活的方式适用这一标准，以方便给予协助。”

70. 第 7 款规定，“本章的规定不限制缔约国之间，或缔约国与服务供应商或其他实体之间，通过其他适用的协议、安排、惯例或国内法进行合作”。这意味着，本议定书并不排除或限制缔约国之间或缔约国与私营实体之间以其他方式开展的任何合作——无论是通过适用的协议、安排、国内法，甚至是非正式的惯例。起草者打算扩大而不是限制执法人员工具箱中的现有工具，以便为具体的刑事调查或诉讼程序获取信息或证据。起草者认识到，在某些情况下，现有机制，如互助，可能是从执业人员的最佳选择。然而，在其他情况下，本议定书创建的工具可能更有效或更可取。例如，如果主管机构需要并非紧急的内容数据，它可能会选择根据双边条约或根据《公约》第 27 条(如适用)，使用传统的互助请求，因为本议定书不包含非紧急情况下获取内容数据的规定。但如果它需要用户信息，可能会选择使用本议定书第 7 条，直接向服务供应商发送命令。

71. 最后，第二章和本议定书其他地方的一些规定允许施加使用限制或条件，例如保密。如果根据本议定书的规定，所要求的证据或资料的接收须受此种使用限制或条件的制约，则谈判者承认有例外情况，这些例外情况也隐含在案文中。首先，作为根据第 13 条保护人权和自由的一项措施，依照许多国家的基本法律原则，如果提供给接收方的材料被接收方认为可以为被告开脱罪责，则必须向被告方或司法当局披露。这一原则不影响第 12 条第 6 款(b)项的案文和解释性报告第 215 段，在缔约国成立了联合调查组的情况下可适用这些案文。起草者的理解是，在这种情况下，接受方将在披露之前通知转交方，并在提出要求时与转交方协商。其次，倘若对根据本议定书收到的预计在审判中使用的材料规定了使用限制，则审判(包括审前司法程序期间的披露)通常属于公开程序。一旦在审判中公开，这些材料就进入了公共领域。在这类情况下，不可能确保为索取的材料的调查或诉讼程序保密。这些例外情况类似

于《公约》解释性报告第 278 段中所解释的与适用《公约》第 28 条第 2 款有关的例外情况。最后，在事先征得转交方同意的情况下，材料可用于其他目的。

第 2 节　加强与其他缔约国供应商和实体直接合作的程序

第 6 条　有关域名注册信息的请求

72. 第 6 条确立了一种程序，规定一缔约国主管机构与在另一缔约国境内提供域名注册服务的实体直接合作，以获得有关互联网域名注册的信息。与第 7 条类似，该程序以《网络犯罪公约》委员会云端证据小组的结论为基础，承认鉴于现有电子证据获取程序所带来的挑战，在具体刑事调查或诉讼中及时跨境获取电子证据的重要性。

73. 该程序还承认当前的互联网监管模式依赖于制定基于共识的多利益主体的政策。这些政策通常以合同法为基础。本条规定的程序旨在为本议定书的目的，即为具体的刑事调查或诉讼的目的，补充这些政策。获取域名注册数据通常是必不可少的，这是许多刑事调查的第一步，也是确定向谁提出国际合作请求的第一步。

74. 犯罪分子出于恶意和非法目的创建和利用域名，为许多形式的网络犯罪提供了便利。例如，域名可能被用作平台传播恶意软件、僵尸网络、网络钓鱼和类似活动、欺诈、分发虐待儿童材料以及其他犯罪目的。因此，获取注册域名的法人或自然人(“注册人”)的信息，对于在具体的刑事调查或诉讼中识别嫌疑人至关重要。虽然域名注册数据历史上是公开的，但现在对其中一些信息的访问受到限制，这影响了司法和执法机关执行公共政策任务。

75. 域名注册信息由提供域名注册服务的实体持有。其中包括向公众出售域名的组织(“注册服务商”)，以及保存顶级域名所有注册域名的权威数据库(“注册管理机构”)并接受注册请求的地区或国家注册管理执行机构。在某些情况下，此类信息可能是个人数据，并有可能受到提供域名注册服务的相关实体(注册服务商或注册管理机构)所在缔约国或数据相关人员所在缔约国的数据保护条例的保护。

76. 第 6 条的目的是提供一个有效和高效的框架，以获取用于识别或联系域名注册人的信息。实施形式取决于缔约国各自的法律和政策考虑。本条旨在补充当前和未来的互联网监管政策和实践。

第 1 款

77. 根据第 1 款，每一缔约国应采取必要措施，授权其主管机构直接向在另一缔约国领土上提供域名注册服务的实体发出请求，即不要求该实体所处领土上的主管机构充当中间人。第 1 款在提出请求的格式方面给予缔约国以灵活性，因为格式取决于缔约国各自的法律和政策考虑。缔约国可使用其国内法规定的程序，包括发布命令；然而，为了第 6 条的目的，这种命令被视为不具有约束力的请求。因此，请求的形式或其根据请求方国内法产生的效力，将不影响本条所规定的国际合作的自愿性质，如果该实体不披露所要求的信息，则应适用第 5 款。

78. 第 6 条第 1 款的措辞范围很广，足以承认也可通过各组织提供的界面、门户或其他技术手段发出此类请求和获取信息。例如，一个组织可以提供一个接口或查询工具，以便于或加快在请求后披露域名注册信息。但是，该条并没有针对任何特定的门户或界面，而是使用了技术中立的术语，以适应技术的不断发展。

79. 正如第 2 条所预见的，根据第 1 款提出的请求，只能为具体的刑事调查或诉讼目的而提出。“主管机构”一词的定义见第 3 条第 2 款(b)项，系指“国内法律授权的司法、行政或其他执法机构，其有权命令、授权或承担执行本议定书项下的措施”。“提供域名注册服务的实体”

目前是指注册服务商和注册管理机构。为了考虑到目前的情况，同时考虑到商业模式和互联网的结构，可能会随着时间的推移而发生变化，本条采用了“提供域名注册服务的实体”这一较通用的术语。

80. 虽然用于识别或联系域名注册人的信息通常由在全球范围内提供一般域名注册服务的实体存储，例如“通用顶级域名”(gTLDs)，缔约国承认，与国家或区域实体有关的更具体的域名注册服务(“国家或地区顶级域名”(ccTLD))也可能被其他国家或地区的个人或实体注册，亦有可能被犯罪分子使用。因此，第 6 条并不局限于提供“通用顶级域名”的实体，因为这两种类型的域名注册服务(或未来的此类服务)都可能被用于实施网络犯罪。

81. 短语“用于识别或联系域名注册人的信息”是指先前通过所谓的 WHOIS 查询工具公开提供的信息，如注册人的姓名、实际地址、电子邮件地址和电话号码。有些缔约国可能认为这种信息是《公约》第 18 条第 3 款所界定的用户信息的一个子集。域名注册信息是基本信息，无法对个人的私生活和日常习惯得出准确的结论。因此，与披露其他类别的数据相比，披露此类数据的侵扰性较小。

第 2 款

82. 第 2 款要求每一缔约国采取措施，允许其领土内提供域名注册服务的实体根据第 1 款的请求披露此类信息，但须遵守国内法规定的合理条件，在某些缔约国，这些条件可能包括数据保护条件。与此同时，第 14 条限制了根据国际数据传输保护规则拒绝数据传输的能力，第 83 段中列入的因素是为了便利根据数据保护规则进行处理。这些措施应尽可能方便以迅速有效的方式披露所要求的数据。

83. 本条并不要求缔约国颁布立法，规定这些实体有义务对另一缔约国官方的请求作出答复。因此，提供域名注册服务的实体可能需要确定是否披露所寻求的信息。本议定书通过提供保障措施协助作出这一确定，这些保障措施应有助于各实体能够毫无困难地答复根据本条提出的请求，例如：

- 本议定书规定或要求缔约国为请求提供法律依据；
- 本条要求请求由主管机构提出(第 6 条第 1 款和第 3 款(a)项，以及本解释性报告第 79 段和第 84 段)；
- 本议定书规定，请求是为了具体的刑事调查或诉讼的目的提出的(第 2 条)；
- 该条要求请求中包含一项声明，说明对信息的需要是由于其与具体的刑事调查或诉讼程序相关，并且该信息将仅用于该特定的刑事调查或诉讼程序(第 6 条第 3 款(c)项)；
- 本议定书通过第 14 条为处理根据此类请求披露和转交的个人数据提供了保障；
- 披露的资料有限，无法就个人私生活得出确切结论；
- 实体可能期望或被要求各按照与互联网名称与数字地址分配机构(ICANN)的合同安排进行合作。

第 3 款

84. 本条第 3 款规定了根据本条第 1 款发出请求的主管机构至少应当提供的信息。该信息对于由提供域名注册服务的实体执行请求特别相关。请求中需要包括：

a. 发出请求的日期以及发出请求的主管机构的身份和联系方式(第 3 款(a)项)(见解释性报告第 79 段)；

b. 所需信息的域名和所需信息的详细清单，包括注册人的姓名、实际地址、电子邮件地址或电话号码等特定数据元素(第 3 款(b)项)；

c. 说明请求是根据本议定书发出的；缔约国作出这一声明即表示该请求符合本议定书的规定(第 3 款(c)项)。请求方还在该声明中确认“需要”该信息缘于它与特定的刑事调查或诉讼有关，并且该信息将仅用于这一具体的刑事调查或诉讼。对欧洲国家来说，刑事调查或诉讼“需要”什么样的信息，即必要和相称的信息，应当从 1950 年《欧洲委员会保护人权与基本自由公约》的原则、其适用的判例以及国家立法和判例中得出。这些来源规定，权力或程序应与犯罪的性质和情节相称(见《网络犯罪公约》解释性报告第 146 段)。其他缔约国将适用其法律的相关原则，如相关性原则(即请求索取的证据必须与侦查或起诉相关)。各方应避免广泛要求披露域名信息，除非是特定刑事调查或诉讼所需；

d. 披露信息的时间和方式以及任何其他特别的程序性指示(第 3 款(d)项)。“特别的程序指示”意在包括任何保密请求，包括不向登记人或第三方披露该项请求的要求。如果需要保密以避免过早披露该事项，则应在请求中加以说明。在一些缔约国，将通过实施法律保持请求的保密性，而在另一些缔约国则不一定如此。因此，在需要保密的情况下，鼓励缔约国在根据第 1 款向提供域名注册服务的实体提出请求之前，审查可公开获得的信息，并就适用法律以及该实体关于用户/注册人信息的政策向其他缔约国寻求指导。此外，特殊程序指令可包括最适合主管机构需要的传输渠道的说明。

85. 第 3 款没有要求在请求中列入事实陈述，因为这一信息在大多数刑事调查中是保密的，不得向私人当事方披露。然而，根据本条收到请求的实体可能需要某些额外信息，以便能够对请求作出积极的决定。因此，该实体可以在无法以其他方式执行该请求的情况下寻找其他信息。

第 4 款

86. 第 4 款的目的是鼓励在提供域名注册服务的实体可以接受的情况下使用电子手段，因为电子手段几乎总是最有效和最快捷的通信手段。因此，如果提供域名注册服务的实体接受，缔约国可通过电子邮件、电子门户网站或其他方式等电子形式向该实体提交请求。虽然假定实体更愿意接受这种形式的请求，但并不要求只能使用这种形式。如本议定书允许以电子形式发出命令或请求的其他条款(如第 7 条、第 8 条及其他条款)所预见的那样，可能需要适当程度的安全和认证。双方和实体可自行决定是否有安全渠道或传输和认证手段，或在特别敏感情况下是否需要特殊的安全保护措施(包括加密)。

第 5 款

87. 虽然本款涉及“请求”，而非披露域名注册数据的强制性“命令”，但如果满足适用条件，则预期被请求实体将能够披露根据本款寻求的信息。如果该实体不披露所寻求的信息，则可根据情况考虑采用其他机制获取该信息。因此，第 5 款规定有关缔约国之间进行协商，以便获得更多的信息和确定现有的机制，例如改进今后的合作。为了便利协商，第 5 款还规定，请求方可要求某一实体提供进一步信息。鼓励各实体解释不披露此类请求所要求的数据的原因。

第 6 款

88. 第 6 款要求，在签署本议定书或交存批准书、接受书或核准书时，或在任何其他时候，各缔约国应指定一个负责根据第 5 款进行协商的机构。在该实体所在缔约国提供一个联络点，将

有助于请求方在该实体拒绝执行根据第 6 条提出的直接请求时，迅速确定可采取哪些措施来获取所要求的数据。

第 7 款

89. 第 7 款是不言自明的，规定欧洲委员会秘书长应建立并保持一份根据第 6 款指定的机构名册，各缔约国应确保为该名册提供的详细内容一向准确无误。

第 7 条 披露用户信息

90. 第 6 条确立了一种程序，规定一缔约国主管机构与在另一缔约国境内提供域名注册服务的实体直接合作，以获取用户信息。该程序以《公约》委员会云端证据小组的结论和《公约》第 18 条指导说明为基础，鉴于从其他国家的服务供应商获取电子证据的现有程序所带来的挑战，承认在具体的刑事调查或诉讼中及时获取跨境电子证据的重要性。

91. 如今，越来越多的刑事调查或诉讼需要从其他国家/地区的服务供应商那里获取电子证据。即使是完全属于国内性质的犯罪——即犯罪、受害人和犯罪人都与调查机关同处一个国家——电子证据也可能由另一国境内的服务供应商持有。在许多情况下，调查犯罪的主管机关可能需要使用国际合作程序，如互助，但由于寻求电子证据的请求数量不断增加，这些程序并非一向能够迅速或有效地提供足够的协助，以满足调查或诉讼的需要。

92. 在与网络犯罪和其他类型需要电子证据的犯罪有关的刑事调查中，最常寻求的信息是用户信息。它提供了某一服务的特定用户的身份、地址以及《公约》第 18 条第 3 款所确定的类似信息。它不允许对有关个人的私生活和日常习惯得出精确的结论，这意味着，与披露其他类别的数据相比，披露这种数据的侵扰程度可能较低。

93. 《公约》第 18 条第 3 款(已纳入本议定书第 3 条第 1 款)将用户信息定义为“以计算机数据形式或任何其他形式存在的、由服务供应商掌握的、有关其服务的用户(除流量或内容数据外)的任何信息，通过这些信息可以确定：(a)所使用的通信服务类型、所采用的技术规定和服务期限；(b)基于服务协议或安排可获得的用户身份、邮政或地理地址、电话和其他接入号码、账单和支付信息；(c)基于服务协议或安排可获得的有关通信设备安装地点的任何其他信息”(另见《公约》解释性报告，第 177 至 183 段)。为识别服务用户而需要的信息可能包括某些互联网协议(IP)地址信息——例如，创建账户时使用的 IP 地址，最近一次登录的 IP 地址或在特定时间使用的登录 IP 地址。在一些缔约国，这种信息由于各种原因被视为流量数据，包括认为它与通信的传输有关。因此，第 7 条第 9 款(b)项为一些缔约国提出了一项保留。

94. 虽然《公约》第 18 条已经述及了需要迅速有效地从服务供应商处获取电子证据的某些方面，但该条本身并没有为这一挑战提供一个完整的解决办法，因为该条适用的情形较为有限。具体而言，《公约》第 18 条适用于服务供应商在签发命令的缔约国“领土上”(见《公约》第 18 条第 1 款(a)项或在签发命令的缔约国境内“提供服务”(见《公约》第 18 条第 1 款(b)项的情况。考虑到第 18 条的局限性和互助所面临的挑战，认为必须建立一个补充机制，以便能够更有效地跨境获取具体的刑事调查或诉讼所需的信息。因此，本议定书第 7 条的范围超出了《公约》第 18 条的范围，因为它允许一缔约国向另一缔约国境内的服务供应商发出某些命令。各缔约国认识到，虽然一缔约国主管机构向另一缔约国的服务供应商发出的这种直接命令对于迅速和有效获取信息是可取的，但不应允许一缔约国利用其国内法下可利用的所有执行机制来执行这些命令。出于这一原因，在服务供应商不披露特定用户信息的情况下，这些命令的执行受到第 7 条第 7 款规定的方式的限制。这一程序规定了保障措施，以考虑到一缔约国官方与另一缔约国服务供应商之间直接合作所产生的独特要求。

95. 如第 5 条第 7 款所反映的，本条不妨碍缔约国执行根据第 18 条或《公约》允许的其他方式发布的命令的能力，也不妨碍缔约国之间或缔约国与服务供应商之间通过其他适用的协定、安排、惯例或国内法进行的合作(包括自发合作)。

第 1 款

96. 第 1 款要求各缔约国授权其主管机构可以发布直接提交给另一缔约国境内的服务供应商的命令，要求其披露用户信息。发布的命令只能针对特定和存储的用户信息。

97. 第 1 款还包括一项要求，即命令只能在发出命令的缔约国本身的“特定刑事调查或诉讼”的背景下发布和提交，正如本议定书第 2 条中使用的这一短语。作为进一步的限制，也可以仅针对调查或诉讼“所需”的信息发布命令。对欧洲国家来说，什么是刑事调查或诉讼所需要的信息——即必要和相称的信息——应缘于1950年《欧洲委员会保护人权和基本自由公约》的原则、其适用的判例以及国家立法和判例。这些来源规定，权力或程序应与犯罪的性质和情节相称(见《网络犯罪公约》解释性报告第 146 段)。其他缔约国应适用其法律的相关原则，如相关性原则(即，命令所寻求的证据必须与调查或起诉相关)和避免披露用户信息的命令过于宽泛的原则。这一限制再次强调了本议定书第 2 条和第 7 条第 1 款已经确立的原则，即该措施仅限于具体的刑事调查和诉讼程序，这些规定不得用于大规模或批量制作数据(另见《公约》解释性报告第 182 段)。

98. “主管机构”一词的定义见第 3 条第 2 款(b)项，系指“国内法律授权的司法、行政或其他执法机构，其有权命令、授权或承担执行本议定书项下的措施”。为本条中的直接合作程序的目的，也设想了同样的方法。因此，一个缔约国的国内法律体系将决定哪个机构被认为是发布命令的主管机构。虽然发出命令的缔约国决定由哪个主管机构可以发出命令，但第 7 条第 5 款规定了一项保障措施，即接收方可以要求指定的主管机构审查根据本条发布的命令，并有权停止直接合作，如下文所述。

99. 在第 7 条中，“另一缔约国境内的服务供应商”一语要求服务供应商实际设在另一缔约国境内。根据该条，例如，服务供应商与某一缔约国的公司建立了合同关系，但服务供应商本身并不在该缔约国境内，这一事实并不构成服务供应商在该缔约国“境内”。此外，第 1 款还要求数据由服务供应商拥有或掌握。

第 2 款

100. 第 7 条第 2 款要求缔约国采取任何必要措施，使其境内的服务供应商对另一缔约国的主管机构根据第 1 款发出的命令作出反应。鉴于国内法律制度的差异，缔约国可以采取不同的措施，建立一种程序，以有效和高效的方式进行直接合作。这可能包括消除服务供应商对命令作出反应的法律障碍，提供肯定答复的依据，使服务供应商有义务以有效和高效的方式对另一方当局的命令作出反应。各缔约国必须以提供法律确定性的方式，确保服务供应商能够合法遵守第 7 条所设想的命令，从而使服务供应商不会因为仅真诚遵守一缔约国根据第 1 款发出的命令而承担法律责任，而该命令是该缔约国声明(依照第 7 条第 3 款(b)项)根据本议定书发出的。这并不排除因遵守命令以外的原因而承担的责任，例如，未能遵守任何适用的法律要求，即服务供应商对存储的信息保持适当的安全水平。实施形式取决于缔约国各自的法律和政策考虑。对于有数据保护要求的缔约国，这将包括为处理个人数据提供明确的依据。鉴于数据保护法对授权最终国际传输回应用户信息的附加要求，本议定书反映了这种直接合作措施的重要公共利益，并在第 14 条中包括了为此目的所需的保障措施。

101. 因此，一个缔约国的国内法律体系将决定哪个机构被视为发布命令的主管机构。一些缔约国认为，鉴于合作的直接性，有必要对命令的合法性作进一步审查(例如，见上文第 98 段)。虽然发布命令的缔约国决定由哪些机构可以发布命令，但第 2 款(b)项允许缔约国作出声明，

表明“第 7 条第 1 款规定的命令必须由检察官或其他司法机关发出，或在其监督下发出，或以其他方式在独立监督下发出”。利用该声明的缔约国必须接受由上述任何一个机构发出的命令或在其监督下发出的命令。

第 3 款

102. 第 7 条第 3 款规定了根据本条第 1 款发出命令的主管机构至少应提供的信息，尽管发出命令的缔约国可以选择在命令中列入补充信息以协助处理，或因为其国内法律要求提供补充信息。第 3 款中规定的信息对于服务供应商执行命令以及服务供应商所在缔约国的主管机构根据第 5 款可能参与其中特别重要。该命令需要包括签发机构的名称和签发日期、辨别服务供应商的信息、属于刑事调查或诉讼标的的罪行、查询用户信息的机构，以及对查找的特定用户信息的详细描述。该命令还须载有一项声明，说明该命令是根据本议定书发出的。该缔约国通过作出这一声明，表示该命令符合本议定书的规定。

103. 关于第 3 款(a)项(签发机构)和第 3 款(e)项(查询用户信息的机构)之间的区别，在一些缔约国，签发机构和查询数据的机构并不相同。例如，调查人员或检察官可能是索取数据的当局，而发布命令的是法官。在这种情况下，必须确定索取数据的机构和签发命令的机构。

104. 考虑到这一信息在大多数刑事调查中是保密的，不得向私人当事方披露，因此不需要对事实加以说明。

第 4 款

105. 虽然第 3 款规定了根据第 1 款发出的命令所需最低限度的信息，但这些命令往往只有在向服务供应商(以及在适用情况下根据第 5 款向接收方的指定机构)提供补充信息时才能执行。因此，第 7 条第 4 款规定，发布命令的机构应提供以下补充信息：授权该机构发布命令的国内法律依据；针对被调查或起诉的犯罪行为的法律规定和适用处罚的说明；服务供应商应向其反馈用户信息，可向其索取进一步信息，或以其他方式对其做出回应的机构的联系方式；反馈用户信息的时限和方式；是否已经要求保存该数据，包括保存日期和任何适用的查询号；任何特别程序指示(例如要求保密或认证)；如适用，说明已按照第 5 款同时发出通知；以及可能有助于获得用户信息披露的任何其他信息。联系方式不需要标识个人，只需标识办公室即可。这种补充信息可以单独提供，但如果签发方的法律允许，也可以包含在命令中。命令和补充信息均应直接发送给服务供应商。

106. 特别程序指示尤其包括任何保密要求，包括不向用户或第三方披露命令的要求，但特别程序指示不得妨碍服务供应商与依据第 5 款(a)项应通知的机构或依据第 5 款(b)项应咨询的机构协商。如果需要保密以避免过早披露该事项，则应在请求中予以说明。在一些缔约国，将通过实施法律维护命令的保密性，而在其他缔约国则不一定如此。因此，为了避免过早披露调查的风险，鼓励缔约国在根据第 1 款向服务供应商提交命令之前，了解适用法律和服务供应商有关用户通知的政策。此外，特别程序指示可包括说明最适合主管机构需要的传输渠道。服务供应商也可以要求提供有关账户的补充信息或其他信息，以有助于其提供迅速和完整的答复。保密要求不应妨碍服务供应商以透明方式报告根据第 7 条收到的命令的匿名总数。

第 5 款

107. 根据第 5 款(a)项，缔约国可通知欧洲委员会秘书长，凡按照第 1 款向其境内的供应商发出命令时，该缔约国要求对每一起事件(即向其境内的服务提供商传送的所有命令)，或在明确注明的情况下，同时获得通知。

108. 根据第 5 款(b)项，一缔约国还可根据其国内法要求，收到另一缔约国命令的服务供应商在标明的情况下与其协商。一方不得要求对所有命令进行协商，这将增加额外步骤，可能造成重大延误，故只能在更为有限和确定的情况下进行协商。协商要求应限于以下情况，即有可能需要施加条件或援引拒绝理由，或担心可能对转交方的刑事调查或诉讼造成损害。

109. 通知和协商程序完全是自由裁量的。一方并无义务要求其中任何一种程序。

110. 根据第 5 款(a)项接获通知或根据第 5 款(b)项被咨询的缔约国，可指示服务供应商基于第 5 款(c)项所述理由不披露信息，涉及第 8 条的解释性报告第 141 段对此作了更详细的说明。正因为如此，缔约国被通知或被咨询的能力获得了一项额外保障。尽管如此，原则上，合作是广泛的，障碍应受到严格限制。因此，正如《公约》解释性报告第 242 和 253 段所解释的那样，由被通知或被咨询的缔约国确定哪些条件和拒绝适用《公约》第 25 条第 4 款和第 27 条第 4 款，也应根据《议定书》第 7 条的目的加以限制，以消除障碍，为跨境获取刑事调查的电子证据提供更有效和快速的程序。

111. 按照第 5 款(d)项，根据第 5 款(a)项发出通知或根据第 5 款(b)项要求咨询的缔约国，可要求第 4 款(c)项所指的主管机构提供补充信息，以确定是否有理由根据第 5 款(c)项指示服务供应商不遵守命令。这一过程将在情况允许的情况下尽快完成。被通知或被咨询的缔约国必须收集必要的信息，并“不得无故拖延”根据第 5 款(c)项作出决定。如有必要，为促进合作，第 5 款(d)项规定的程序还可提供机会，澄清所寻求的信息的保密性，以及寻求数据的机构的任何预期用途限制。该缔约国还必须在其决定指示服务供应商不遵守的情况下迅速通知发布方的主管机构，并提供这样做的理由。

112. 要求通知或咨询的缔约国，可决定在服务供应商根据命令提供用户信息之前，对其规定一个等待期，以便允许通知或咨询以及该缔约国对补充信息的任何后续要求。

113. 根据第 5 款(e)项，要求通知或咨询的缔约国必须指定一个单一的机构，并在根据第 5 款(a)项要求通知时，向欧洲委员会秘书长提供充分的联系方式。

114. 一方可随时更改其通知或咨询要求，具体取决于其对任何相关因素的判断，例如，其是否希望从通知制度转向咨询制度，或其是否已通过直接合作达到足够的满意程度，可以修改或取消之前的通知或咨询要求。同样，它亦可以根据直接合作机制的经验，决定是否希望设立一个通知或咨询制度。

115. 根据第 5 款(f)项，欧洲委员会秘书长需要建立并保持一个缔约国根据第 5 款(a)项和 5 款(e)项提出的通知要求的最新名册。拥有一个公开的最新名册对于确保发出通知的缔约国的主管机构和服务供应商了解各缔约国的通知要求至关重要，如上所述，这些要求可以随时改变。由于各缔约国可自行决定作出此类变更，因此，各缔约国如果对其在名册中的细节作出任何更改，或注意到任何不准确之处，都必须立即通知秘书长，以确保其他缔约国都了解目前的要求并能正确适用这些要求。

第 6 款

116. 第 6 款明确规定，允许使用电子形式通知另一缔约国并提供补充信息，包括使用电子邮件和电子门户网站。如果服务供应商接受，缔约国可以电子形式提交第 1 款所述的命令和第 4 款所述的补充信息。第 4 款的目的是鼓励在提供域名注册服务的实体可以接受的情况下使用电子手段，因为电子手段几乎一向是最有效和最快捷的通信手段。认证方法可包括允许安全识别请求机构的各种手段或其组合。这些手段可包括，例如，通过发文方的一个已知机构(例如来自发文方或中央机关或指定机构)获得真实性确认，发文方和收文方之间的后续通信，使用官方电子邮件地址或发文方可轻易使用的未来技术验证方法。第 10 条第 2 款载有类似的

条文，解释性报告第 174 段提供了关于担保要求的进一步指导。本议定书第 6 条第 4 款和第 8 条第 5 款也载有类似的条文。

第 7 款

117. 第 7 款规定，如果服务供应商不遵守根据第 7 条发出的命令，发出命令的缔约国只能根据第 8 条或另一种互助形式寻求命令得以执行。根据该条履行程序的当事方不得寻求单方面执行。

118. 为了借助第 8 条执行命令，本议定书设想了将本条下的命令转换为第 8 条下的命令的简化程序，以方便发布方获得用户信息的能力。

119. 为避免重复工作，发布方必须给服务供应商 30 天或第 4 款(d)项规定的时间限度(以时间较长者为限)，以便履行通知和咨询程序，并让服务供应商披露信息或表明拒绝披露。只有在该期限届满后，或如果供应商在该期限届满前表示拒绝遵守，发布方才可根据第 8 条或其他互助形式寻求执行。为了使主管机构能够评估是否根据第 7 款寻求强制执行，鼓励服务供应商解释为何不提供所寻求的数据的理由。例如，服务供应商可以解释数据不再可用。

120. 根据第 5 款(a)项接获通知或根据第 5 款(b)项被咨询的主管机构已通知发布方，业已指示服务供应商不得披露所寻求的信息，发布方仍可通过第 8 条或其他互助形式的寻求执行命令。然而，这种进一步的请求有可能同样被拒绝。建议发布方事先与第 5 款(a)项或第 5 款(b)项指定的主管机构协商，以解决最初命令中的任何缺陷，并避免根据第 8 条或通过任何其他互助机制提交可能被拒绝的命令。

第 8 款

121. 根据第 8 款，一缔约国可宣布另一缔约国在根据第 8 条要求披露用户信息之前，应向服务供应商寻求披露用户信息，除非发出命令方对没有这样做的理由给出合理解释。例如，一缔约国可以作出这样的声明，因为它认为本条规定的程序应使其他缔约国能够比动用第 8 条规定的程序更快地获得用户数据，从而可以减少需要援引第 8 条的情况。第 8 条规定的程序仅在以下情况下使用：直接从服务供应商处寻求披露用户信息的尝试未果；发布方有合理的理由不首先使用本条规定；或发布方保留不适用本条规定的权利。例如，当服务供应商通常不提供用户信息作为对直接从发布方收到的命令作出回应时，发布方可以证明这一点。或者，作为另一个例子，如果发布方通过一项单一的命令从另一个对两类数据都适用第 8 条的缔约国寻求用户信息和流量数据，发布方将不需要首先单独寻求用户信息。

第 9 款

122. 根据第 9 款(a)项，对本条持保留意见的缔约国无需根据第 2 款采取措施，要求其境内的服务供应商根据其他缔约国发出的命令披露用户信息。对本条持保留的缔约国不得根据第 1 款向其他缔约国境内的服务供应商发出命令。

123. 第 9 款(b)项规定——出于上文第 93 段所述理由——如果缔约国根据本条披露某些类型的访问代码与其国内法律制度的基本原则相抵触，可以保留不将本条适用于此类代码的权利。对本条持保留的缔约国不得根据第 1 款向其他缔约国境内的服务供应商发出命令。

第 3 节　加强官方机构之间就披露存储的计算机数据开展国际合作的程序

第 8 条　执行另一方关于加快提供用户信息和流量数据的命令

124. 第 8 条的目的是让请求方作为向另一缔约国提出请求的一部分，有能力发布命令，并让被请求方有能力执行该命令，迫使其境内的服务供应商提供其拥有或掌握的用户信息或流量数据。

125. 该条建立了一个补充《公约》互助条款的机制。它旨在比目前的互助更为精简，缘于请求方须提供的信息更有限，获取数据的过程更迅速。本条是对《公约》或其他多边或双边协定规定的其他互助程序的补充，因此并不妨碍缔约国仍然可以自由援引这些程序。事实上，在请求方希望从对第 8 条这一方面持有保留的缔约国寻求流量数据的情况下，请求方可使用另一种互助程序。通常情况下，如果同时寻求用户信息、流量数据和存储内容数据，通过单一的传统互助请求寻求同一账户的所有三种形式的数据，而不是通过本条规定的方法寻求某种类型的数据和通过单独的互助请求寻求其他类型的数据，效率可能会更高。

第 1 款

126. 第 1 款要求请求方能够发出命令，从另一缔约国境内的服务供应商那里获得用户信息或流量数据。第 8 条所指的“命令”是指任何旨在迫使服务提供商提供用户信息或流量数据的法律程序。例如，它可以通过出示令、传票或其他法律授权的机制来执行，并且可以为强制出示用户信息或流量数据而发布。

127. 根据第 3 条第 2 款(b)项的定义，该条第 1 款中的“主管机构”系指国内法律授权的司法、行政或其他执法机构，其有权命令、授权或承担执行本议定书项下的措施，以收集或出示与具体刑事调查或诉讼有关的证据。应当指出的是，根据第 1 款发布命令的主管机构不一定与根据第 8 条第 10 款(a)项指定提交命令以使其生效的机构相同，下文将对此作出更详细的说明。

128. 在第 7 条中，“另一缔约国境内的服务供应商”一语要求服务供应商于另一缔约国境内实际存在。根据该条，例如，服务供应商与某一缔约国的公司建立了合同关系，但服务供应商本身并不设在该缔约国境内，这一事实并不构成服务供应商在该缔约国“境内”。此外，第 1 款还要求数据由服务供应商拥有或掌握。

第 2 款

129. 第 2 款要求被请求方采取必要措施，在其境内执行根据第 1 款发出的命令，但须遵守下文所述的保障措施。“生效”是指被请求方将强迫服务供应商使用被请求方选择的机制提供用户信息和流量数据，但此机制须使该命令可根据被请求方的国内法执行，并符合本条的要求。例如，被请求方可以通过接受请求方的命令，使其与国内命令具有同等效力，通过认可请求方的命令，使其具有与国内命令相同的效力，或发出自己的出示令，使请求方的命令生效。任何这类机制将受被请求方法律条款的制约，因为被请求方的程序将控制这类机制。因此，被请求方可确保其本国法律，包括宪法和人权要求得到满足，特别是在任何额外保障方面，包括提供流量数据所需的保障。

130. 虽然本条可通过若干方式得到遵守，但缔约国不妨设计自己的内部程序，使之能够灵活处理来自各主管机构的请求。谈判第 3 款(b)项是为了确保向被请求方提供充分的信息，以确保在需要时能够进行全面审查，因为一些缔约国表示，它们将发布自己的命令，作为使请求方的命令生效的一种方式。

第 3 款

131. 为启动被请求方执行命令的程序，请求方应转交命令及证明资料。第 3 款描述了请求方必须向被请求方提供的内容，以便被请求方能执行命令并强制其境内的服务供应商予以提供。第 3 款(a)项描述了应列入命令本身的信息，包括对执行命令至关重要的信息。第 3 款(b)项中的信息仅供被请求方使用，除非得到请求方的同意，否则不得与服务供应商分享，这些信息

是证明该命令的国内法律依据和本议定书中的国际依据的佐证资料，并为被请求方评估第 8 款规定的条件或拒绝的潜在理由提供参考。缔约国在根据第 8 条提出请求时，应说明是否有第 3 款(b)项所述的任何信息可与服务供应商分享。根据第 3 款(c)项，请求中还应包括所有特别指示，包括例如对请求的认证或保密要求(类似于《公约》第 27 条第 8 款)，在传送时确保请求得到妥善处理。

132. 第 3 款(a)项所述的用户信息或流量数据的命令必须在字面上指明:(1)签发命令的机构和签发日期；(2)一份根据本议定书签发命令的说明；(3)将要送达的服务供应商的名称和地址；(4)属于刑事调查或诉讼标的的罪行；(5)查询数据的机构或者是签发机构；(6)对所查询的具体数据的详细描述(即用户的身份、邮政或地理地址、电话或其他接入号码，以及根据服务协议或安排提供的账单和付款信息(见包含《公约》第 18 条第 3 款的本议定书第 3 条和上述解释性报告第93段))；关于流量数据，与通过计算机系统进行的通信有关的计算机数据，由构成通信链的一部分的计算机系统产生，表明通信的来源、目的地、路线、时间、日期、规模、持续时间或基本服务的类型(见本议定书第 3 条第 1 款，其中包含《公约》第 1 条(d)项)。关于第 3 款(a)项(5)目，如果签发机构与查询数据的机构非同一机构，则该款项要求两者都要明确身份。例如，一个调查或起诉机构可能正在查询数据，而发布命令的是法官。这一信息表明了命令的合法性，并为其执行提供了明确的指示。

133. 第 3 款(b)项所述的证明资料旨在向被请求方提供执行请求方的命令所需的参考。这也可以通过一个易于填写的模板来实现，这可以进一步提高流程的效率。证明资料清单可包括以下内容：

第 3 款(b)项(1)目提到了赋予发布机关有权发出强制出示令的法律依据。换言之，这是授权主管机构发布第 1 款所述命令的相关法律。

第 3 款(b)项(2)目提到了与第 3 款(a)项(4)目的命令中提到的罪行有关的法律规定及其相关的处罚范围。列入这两项内容对于被请求方评估该请求是否属于其义务范围之事十分重要。

第 3 款(b)项(3)目提及请求方能够提供的任何信息，这些信息使其得出结论认为，作为命令主体的服务供应商拥有或掌握着所寻求的信息或数据。这一信息是被请求方启动这一进程的关键。查明国内服务供应商并相信其拥有或掌握所寻求的信息或数据往往是启动出示令申请的先决条件。

第 3 款(b)项(4)目提及与调查或诉讼有关的事实概要。这一资料也是被请求方确定是否应在其领土上执行该条所指命令的一个关键因素。

第 3 款(b)项(5)目提及关于信息或数据与调查或诉讼相关联的声明。这一声明是为了帮助被请求方确定本条第 1 款的要求是否得到满足，即有关资料或数据是“该缔约国特定刑事调查或诉讼所需的”。

第 3 款(b)项(6)目提及一个或多个机构的联系方式，以备被请求方的主管机构要求提供更多信息以执行命令。

第 3 款(b)项(7)目提及关于是否要求保全该信息或数据的情况。这一信息对被请求方来说十分重要，特别是与流量数据有关的信息，应包括例如查询号码和保存日期，因为这一信息可使被请求方将目前的请求与以前的保全请求加以匹配，从而有利于披露最初保全的信息或数据。为了减少信息或数据被删除的风险，鼓励缔约国在根据本条提出请求之前，尽快设法保全所寻求的信息或数据，并设法及时延长保全期限。

第 3 款(b)项(8)目提及是否已经通过其他方式寻求数据的情况，如果是，以何种方式寻求。这一规定主要涉及请求方是否已经直接从服务供应商处寻求用户信息或流量数据。

134. 根据第 3 款(b)项提供的信息，未经请求方同意，不得向服务供应商披露。特别是，向被请求方提供关于信息或数据与调查或诉讼程序关联情况的事实摘要和说明，以确定是否有理由施加条件或予以拒绝，但通常受调查保密性的限制。

135. 根据第 3 款(c)项，请求方可要求执行特殊的程序性指示，包括要求不向用户披露命令或作为证据而填写的核证表格。由于特殊指示可能需要被请求方内部履行额外的程序，因此必须在一开始就了解这一信息。

136. 为了使命令生效，并进一步促进信息或数据的出示，被请求方可向服务供应商提供其他信息，如出示方法，以及在被请求方应向和何人出示数据。

第 4 款

137. 根据第 4 款，可能需要向被请求方提供补充资料，以便其执行命令。例如，根据一些缔约国的国内法，提供流量数据可能需要进一步的信息，缘于其法律对获取此类数据有额外的要求。此外，被请求方可能要求对根据第 3 款(b)项提供的信息作出澄清。另一个例子是，如果命令不是由请求方的检察官或其他司法或独立行政机关签发或审查的，一些缔约国可能要求提供额外的信息。在作出此类声明时，缔约国应尽可能具体地说明所需进一步信息的类型。

第 5 款

138. 第 5 款要求被请求方接受电子形式的请求。它可能要求使用安全和可以认证的电子通信手段，以方便信息或数据和文件的传输，包括命令和辅助信息的传输。第 6 条至第 11 条也预见到这种通信手段。

第 6 款

139. 根据第 6 款，被请求方应采取合理步骤，迅速处理请求。被请求方应尽合理努力处理请求，在被请求方收到所有必要的文件和资料后 45 天内处理请求，并让服务供应商送达。被请求方应命令服务供应商在 20 天内提供用户信息，在 45 天内提供流量数据。虽然被请求方应寻求尽快强制提供，但有许多因素可能会延迟提供，如服务供应商反对，不答复请求或不满足提供的反馈日期，以及可能要求被请求方处理的请求数量过多。因此，决定要求被请求方做出合理努力，只完成其所掌控的程序。

第 7 款

140. 缔约国承认，如果被请求方的一些特别程序指示需要额外的国内程序以落实特别程序指示，也可能造成处理命令的延误。被请求方还可能要求请求方提供额外的信息，以支持任何补充命令的申请，例如保密命令(不披露命令)。根据被请求方的法律，有些程序性指示可能无法使用，在这种情况下，第 7 款规定，被请求方应及时通知请求方，并说明可以遵守的任何条件，使请求方有能力决定是否愿意继续执行该请求。

第 8 款

141. 根据第 8 款，如果存在《公约》第 25 条第 4 款或第 27 条第 4 款规定的拒绝理由，被请求方可以拒绝执行一项请求。例如，根据《公约》解释性报告第 257 段，这一条规定须以适用的互助条约和国内法中规定的拒绝理由为准，并规定了“为在被请求方境内的人提供了权利保

障”，而根据该解释性报告第 268 段，可以“损害国家主权、安全、公共秩序或其他基本利益”为理由，拒绝提供协助。被请求方还可以规定允许执行请求所必需的条件，例如保密。此外，被请求方可以根据《公约》第 27 条第 5 款推迟执行请求。被请求方应将其拒绝、有附加条件或推迟执行请求的决定通知请求方。此外，缔约国可根据《公约》第 28 条第 2 款(b)项的规定适用使用限制。

142. 为了促进提供最广泛合作措施的原则(见第 5 条第 1 款)，被请求方提出的拒绝理由的范围应当狭窄，并且应当有所克制。应回顾《公约》解释性报告第 253 段规定，“相互援助原则上应是广泛的，其障碍应受严格限制”。因此，还应根据本条的目的，对条件和拒绝加以限制，以消除跨界共享用户信息和流量数据的障碍，并提供比传统互助更高效快捷的流程。

第 9 款

143. 根据第 9 款，“如果请求方不能遵守被请求方根据第 8 款提出的条件，应及时通知被请求方。然后，被请求方应决定是否仍提供该信息或材料。如果请求方接受该条件，则应受其约束。.....被请求方，可要求请求方就该条件解释对该信息或材料的使用情况”。

第 10 款

144. 第 10 款的目的是确保各缔约国在签署或交存批准书、接受书或核准书时，指明根据第 8 条提交和接受命令的官方机构。缔约国不必提供具体个人的姓名和地址，但可以指明被认为有能力根据本条发出和接收命令的办公室或单位。

第 11 款

145. 第 11 款允许一缔约国声明，要求其他缔约国依照本条提出的请求，须由请求方的中央机关或由当事双方共同决定的其他机关提交给它。鼓励缔约国在提交请求方面尽可能表现出灵活性。

第 12 款

146. 第 12 款要求欧洲委员会秘书长建立并持续更新缔约国根据第 10 款指定的机构名册，并要求各缔约国应确保为该名册提供的详细内容一向准确无误。此类信息将有助于被请求方核实请求的真实性。

第 13 款

147. 根据第 13 款，保留对流量数据不适用本条权利的缔约国，不需要执行另一缔约国关于流量数据的命令。Dui 本条规定持有保留的缔约国不得根据第 1 款向其他缔约国提交流量数据的命令。

第 9 条 紧急情况下快速披露存储的计算机数据

148. 除了本议定书规定的其他快速合作形式外，起草者意识到，需要促进缔约国在紧急情况下迅速获得另一缔约国境内的服务供应商所拥有或掌握的特定存储计算机数据的能力，以用于特定的刑事调查或诉讼。如本解释性报告第 42 和 172 段所述，在各种紧急情况下，可能需要最大限度地加快合作，例如在恐怖袭击发生后的第一时间，可能使医院系统瘫痪的勒索软件攻击时，或在调查绑架者用来发出要求和与受害者家人联系的电子邮件账户时。

149. 按照《公约》，在紧急情况下，缔约国为获取数据提出互助请求，依照《公约》第 35 条第 1 款(c)项，全天候(24/7)网络可为执行此类请求提供便利。此外，一些国家的法律制度允许其他国家的主管机构通过全天候(24/7)网络寻求紧急披露数据，而无需发送互助请求。

150. 如第 5 条第 7 款所体现的，不妨碍缔约国之间或缔约国与服务供应商之间通过其他适用的协定、安排、惯例或国内法进行合作(包括自发合作)。因此，根据本议定书，在紧急情况下寻求数据的主管机构仍然可以使用上述所有机制。本议定书的创新之处在于拟订了两项条款：第 9 条和第 10 条，规定所有缔约国至少有义务提供具体渠道，以便在紧急情况下迅速开展合作。

151. 该条允许缔约国在紧急情况下利用《公约》第 35 条建立的全天候(24/7)网络作为渠道合作获取计算机数据。全天候(24/7)网络特别适合于处理本条所设想的时间紧迫和高度优先的请求。在实践中，这些联络点可以快速沟通，无需书面翻译，并且能够兑现收到的其他缔约国的请求，无论是直接向其境内的供应商提出请求，还是向其他主管机构寻求的协助，或者根据该缔约国的国内法要求向司法机关提出的请求。这些联络点还可以就请求方可能遇到的涉及供应商和电子证据收集的问题提供建议，例如，解释获取证据必须满足的国内法。这种双向沟通可以增强请求方对被请求方国内法的理解，并有助于较为顺利地获取所需要的证据。

152. 使用本条建立的渠道可能比第 10 条规定的紧急互助渠道更具优势。例如，这种渠道的优点是不需要预先准备互助请求。可能需要相当长的时间来事先编写互助请求，作出翻译并通过国内渠道转交请求方的中央互助机构，而第 9 条并不要求这样做。此外，一旦被请求方收到请求，倘若必须获得补充资料才能给予协助，则相互协助请求可能需要额外时间，更有可能减缓请求的执行。在相互协助方面，被请求方往往要求以书面和更详细的形式提供补充信息，而全天候(24/7)渠道则利用实时信息交流运作。另一方面，紧急互助渠道在某些情况下具有优势。例如，(1)如果有关中央机关之间有特别密切的工作关系，使用该渠道可能少有或没有时间损失；(2)紧急互助可用于获得供应商所掌握的计算机数据以外的其他形式的合作；(3)通过互助获得的证据可能更容易认证。应由缔约国根据其积累的经验和手头的具体法律和事实情况，决定在具体案件中使用哪一种渠道更好。

第 1 款

153. 根据第 1 款(a)项，各缔约国应采取必要的措施，确保其全天候(24/7)网络联络点能够在紧急情况下向另一缔约国的联络点发送请求，请求立即提供协助，并接受其他缔约国联络点对该缔约国境内供应商所掌握的特定存储的计算机数据提出的请求。按照第 2 条的规定，必须根据具体的刑事调查或诉讼程序提出请求。

154. 如上文解释报告第 152 段所述，全天候(24/7)网络联络点必须有能力在紧急情况下传送和接收此类请求，而不必事先准备和传送互助请求，但有可能根据第 9 条第 5 款做出声明。“紧急情况”一词的定义见第 3 条。根据第 9 条，被请求方应利用第 3 款所提供的信息确定是否存在与请求有关的“紧急情况”。

155. 与本议定书中的其他条款如第 7 条仅可用于获取“特定存储的用户信息”不同，本条使用了范围更广的术语“特定存储的计算机数据”。该术语的范围很广，但并非不加区别：它涵盖《公约》第 1 条(b)项所界定的任何“特定”计算机数据，该款已纳入本议定书第 3 条第 1 款。使用这一较宽泛的术语，是承认在紧急情况下获取存储的内容和流量数据，而不仅仅是用户信息的重要性，但并不要求将提交互助请求作为前提条件。所指的数据是存储的或现有的数据，不包括尚未出现的数据，例如与未来通信相关的流量数据或内容数据(见《公约》解释性报告第 170 段)。

156. 这一规定为请求方提供了灵活性，使其能够根据本国法律确定应由其哪个官方机构提出请求，例如进行调查的主管机构或其联络点。然后，请求方的全天候(24/7)网络联络点作为渠道，将请求传递给另一缔约国的全天候(24/7)联络点。

157. 根据第 1 款(b)项，缔约国可声明，将不执行第 9 条下仅为《公约》第 18 条第 3 款所界定并纳入本议定书第 3 条第 1 款的用户信息提出的请求。对一些缔约国来说，根据本条仅接收关于用户信息的请求可能会使全天候(24/7)网络联络点负担过重，因为这会将资源和精力从内容或流量数据请求转移到其他方面。在这种情况下，仅要求提供用户信息的缔约国可转而使用第 7 条或第 8 条，因为这两条有利于迅速披露此类信息。此类声明并不禁止其他缔约国在根据本条要求提供内容和(或)流量数据时也要求提供用户信息。

第 2 款

158. 第 2 款要求每一缔约国采取必要措施，确保其主管机关能够根据国内法向境内的服务供应商索取并获得根据第 1 款要求的数据，并对这种请求作出回应，而无需请求方提出互助请求，但可以依照第 5 款作出声明。

159. 考虑到各国法律的差异，第 2 款旨在为缔约国提供灵活性，构建对第 1 款之下的请求作出答复的系统。然而，鼓励缔约国制定遵守本条规定的机制，重视速度和效率，适应紧急情况的需要，并为在紧急情况下向其他缔约国披露数据提供广泛的法律依据。

160. 被请求方可自行决定：(1)是否满足使用本条的要求；(2)另一种机制是否适合协助请求方；(3)执行全天候(24/7)网络联系点收到的请求的适当权威性。虽然一些缔约国的全天候(24/7)网络联络点本身可能已拥有执行请求的必要权力，但其他缔约国可能要求其联络点将请求转交给另一个或多个机构，以寻求供应商披露数据。在一些缔约国，这可能需要获得司法令以寻求披露数据。被请求方还可自行决定向请求方传送应答数据的渠道，无论是通过全天候(24/7)联络点还是通过另一个机构。

第 3 款

161. 第 3 款具体规定了根据第 1 款提出的请求中应提供的信息。第 3 款规定的信息是为了方便被请求方的相关机构审查并在适当情况下执行该请求。

162. 关于第 3 款(a)项，请求方应具体说明索取数据的主管机构。

163. 关于第 3 款(b)项，请求方必须说明其请求是根据本议定书提出的。这将保证该请求符合本议定书的规定，并保证因此而收到的任何数据将以符合本议定书要求的方式处理。这也将该请求与全天候(24/7)网络联系点可能收到的其他紧急披露请求区分开来。

164. 根据第 3 款(e)项，请求方必须提供充分的事实，证明存在第 3 条所界定的紧急情况，并证明请求所要求的数据与该紧急情况的关系。如果被请求方要求对请求作出澄清，或要求提供补充资料，以便就请求采取行动，则应与请求方的全天候(24/7)网络联络点进行协商。

165. 根据第 3 款(g)项，请求应说明任何特殊的程序性指示。其中特别包括要求不向用户和第三方披露请求，或要求为所寻求的数据填写认证表格。根据本款，这些程序性指示是在一开始就提供的，因为特别指示可能需要在被请求方内部有额外的程序。在某些缔约国，保密性可通过实施法律予以维护，而在其他缔约国，则不一定如此。因此，为了避免过早披露调查情况的风险，鼓励缔约国就保密的必要性和可能出现的任何困难进行沟通，包括任何适用的法律以及服务供应商关于通知的政策。由于对回应数据的认证请求往往会阻碍迅速披露所寻求

数据这一关键目标，被请求方官方机构应与请求方官方机构协商，确定何时和以何种方式提供真实性确认。

166. 此外，缔约国或服务供应商可要求提供额外的信息，以查找和披露请求方寻求的已存储的计算机数据。

第 4 款

167. 第 4 款要求被请求方接受电子形式的请求。鼓励缔约国使用快速通信手段，以方便信息或数据和文件的传输，包括请求的传输。本款以第 8 条第 5 款为基础，但作了修改，增加了缔约国可以接受口头请求，这是全天候(24/7)网络常用的一种通信方法。

第 5 款

168. 第 5 款允许一缔约国作出声明，要求根据本条向其索取数据的其他缔约国在执行请求和传送数据后，以特定的格式和通过特定的渠道，提供请求和为支持请求而传送的任何补充信息。例如，一缔约国可宣布，在特定情况下，它将要求提出请求的缔约国随后提交互助请求，以便正式记录下紧急请求和事先决定提供数据以回应这种请求。有些缔约国的国内法要求采用这种程序，而另一些缔约国则表示，它们没有这种要求，也不需要利用这种可能性作出声明。

第 6 款

169. 本条提及“请求”，并不要求被请求方向请求方提供所请求的数据。因此，起草者承认，在某些情况下，被请求方将不会根据本条向请求方提供所要求的数据。被请求方可决定在特定情况下，根据第 10 条提供紧急互助或另外一种合作方式更为恰当。因此，第 6 款规定，如果被请求方决定不向根据本条第 1 款提出请求的缔约国提供所要求的数据，被请求方应迅速将其决定通知请求方，并在适用的情况下，须指明在何种条件下会提供数据，并解释可能提供的任何其他合作形式，以努力实现缔约国在紧急情况下加快披露数据的共同目标。

第 7 款

170. 第 7 款描述了被请求方对根据第 6 款给予合作规定了具体条件的情况下的适用程序。根据第 7 款(a)项，如果请求方不能遵守规定的条件，它必须立即提请被请求方注意这一情况，而后被请求方应决定是否仍然可以给予协助。相反，如果请求方已接受某项特定条件，则应受该条件的约束。根据第 7 款(b)项，按照第 6 款规定的条件提供信息或材料的被请求方，为确定该条件是否得到遵守，可要求请求方解释它对所提供信息或材料的使用情况，但有一项谅解，请求方不得要求作出过于繁琐的说明(见《公约》解释性报告第 279 和 280 段)。

第 4 节　关于紧急互助的程序

第 10 条　紧急互助

171. 本议定书第 10 条旨在为紧急情况下提出的互助请求提供一种快速程序。第 3 条第 2 款(c)项对紧急情况作了界定，本解释性报告相关的第 41 和 42 段对此作了解释。

172. 由于本议定书第 10 条仅限于有理由采取此种迅速行动的紧急情况，因此与《公约》第 25 条第 3 款有所不同，后者规定，在未达到所界定的紧急程度的紧急情况下，可通过快速通信手段提出互助请求。换句话说，第 25 条第 3 款的范围比本议定书第 10 条更广，因为它涵盖了第 10 条未涵盖的情况，例如对生命或人身安全的持续但并非迫在眉睫的危险、可能由于拖延而导致的证据可能灭失、审判日期迅速临近或其他类型的紧急情况。虽然第 25 条第 3 款中

的机制规定了一种更迅速转达和答复请求的方法，但在紧急情况下，本议定书第 10 条所规定的义务要大得多；即在自然人的生命或安全面临重大和迫在眉睫的危险时，这一进程甚至更应加快(紧急情况的例子见本解释性报告第 42 段)。

第 1 款

173. 根据第 1 款，在提出紧急请求时，请求方必须得出结论，认为存在第 3 条第 2 款(c)项所指的紧急情况，并在请求中说明印证这一点的事实，解释所寻求的协助对于应对紧急情况的必要方式，以及根据适用的条约或被请求方的国内法要求在请求中包含的其他信息。在这方面，应当回顾，根据《公约》第 25 条第 4 款，执行互助请求一般“须符合被请求方的法律或适用的互助条约所规定的条件，包括被请求方可拒绝合作的理由”。起草者的理解是，这也适用于根据本议定书提出的紧急互助请求。

第 2 款

174. 第 2 款要求被请求方接受电子形式的互助请求。在接受请求之前，被请求方可将请求方遵守适当级别的安全和认证作为接受请求的条件。关于本款中的安全要求，缔约国可自行决定是否有必要在特别敏感的情况下采取特别的安全保护措施(包括加密)。

第 3 款

175. 如果被请求方需要更多的信息以得出结论，认为发生了第 3 条第 2 款(c)项所指的紧急情况和(或)其他互助请求已得到满足，则第 3 款要求被请求方迅速寻求更多的信息。同样，第 3 款要求请求方以同样迅速的方式提供补充信息。因此，双方应尽最大努力避免浪费时间，以免无意中造成悲剧性结果。

第 4 款

176. 根据第 4 款，一旦提供了执行请求所需的信息，被请求方即须以同样迅速的方式对请求作出答复。这通常意味着加快速度获得司法命令，迫使供应商提供作为犯罪证据的数据，并同样迅速地向供应商送达命令。然而，供应商回应此种命令时间上的延误，不应归咎于被请求方的官方机构。

第 5 款

177. 根据第 5 款，各缔约国应确保其中央机关或负责答复互助请求的其他机关的成员每周 7 天每天 24 小时随时待命，以防需要在正常办公时间以外提出紧急互助请求。应当回顾，在这方面，《公约》第 35 条规定的全天候(24/7)网络可用于与负责相互协助的机关进行协调。本款规定的义务并不要求负责对互助请求作出回应的中央机关或其他机关在任何时候都备有工作人员和运作。相反，该机构应执行程序，确保可以联系到工作人员，以便在正常工作时间以外审查紧急请求。《公约》委员会将努力非正式地保持一个这类机构的目录。

第 6 款

178. 第 6 款为负责互助的中央机关或其他机关提供了基础，以便共同确定传送响应信息或证据的替代渠道(无论是传送方式，还是双方的传送机关)。因此，与其通过通常用于传送在执行请求方请求时提供的信息或证据的中央机关渠道发回答复信息或证据，双方可共同决定使用不同的渠道，以加快传送速度，保持证据的完整性或出于其他原因这样做。例如，在紧急情况下，官方机构可决定将证据直接传送给请求方将使用该证据的调查或起诉机构，而不是通过该证据通常会经过的一系列机构。例如，官方机构还可以决定对物证进行特殊处理，以便能

够在随后的司法程序中排除对证据可能被篡改或污染的质疑，或者可以共同决定对敏感证据的传送进行特殊处理。

第 7 款

179. 关于本条规定的程序，如第 7 和第 8 款所述，有两种可能性。第 10 条第 7 款规定，当有关缔约国不受基于统一或对等立法订立的适用互助协议或安排相互约束时，缔约国适用《公约》第 27 和第 28 条(关于在无条约情况下的互助)的具体各款规定的某些程序。

第 8 款

180. 第 8 款规定，当有关缔约国受此类协议或安排相互约束时，第 10 条由该协议或安排的规定予以补充，除非有关缔约国相互决定适用第 7 款所述《公约》的任一或所有规定以取代该协议或安排。

第 9 款

181. 最后，第 9 款规定了发表声明的可能性，本议定书缔约国可依据此规定由检察官或其他司法机关彼此之间直接提出请求。在一些缔约国，这种司法机关之间的直接渠道业已建立，可为进一步加快提出和执行请求提供一种有效的手段。通过缔约国的全天候(24/7)联络点或借助国际刑事警察组织(刑警组织)传送紧急请求，不仅有助于减少任何延误，而且有助于提高安全和认证标准。然而，在一些缔约国，在没有中央机关参与和批准的情况下，直接向被请求方的司法机构发出请求可能会产生反效果，因为没有中央机关的指导和(或)批准，接收机构可能无权独立行事，或者可能不熟悉适当的程序。因此，缔约国必须声明可通过这些非中央机关的渠道发送请求。

第 5 节　在无适用的国际协议的情况下有关国际合作的程序

182. 恰如第 5 条第 5 款阐明的，本节与第 11 条和第 12 条有关，它适用于“在请求方与被请求方之间不存在以统一或对等立法为基础的互助条约或安排的情况”。除第 12 条第 7 款另有规定外，第 5 节的规定不适用于存在此种条约或安排的情况。然而，有关缔约国可相互决定适用第 5 节的规定，以代替现有的条约或安排，除非条约或安排的中规定禁止此举。这遵循了《公约》第 27 条的做法。

183. 在本议定书的一些缔约国之间，第 11 条和第 12 条的主题已通过互助条约的条款得以规范(例如《欧洲刑事事项互助公约第二附加议定书》(《欧洲条约集》第 182 号)或《欧洲联盟与美利坚合众国之间的司法互助协定》)。诸如《欧洲条约集》第 182 号等互助条约也可就开展此类合作的情况、条件和程序作出更详细的规定。

184. 虽然起草者考虑到了这些条约，但本议定书第 11 条和第 12 条所载的用语与其他互助条约中的类似规定有所不同。

185. 虽然《欧洲条约集》第 182 号的条款将继续在缔约国之间适用，据认为本议定书中在某些方面以有所不同的方式对这两条加以规范较为妥当，其原因如下：

《欧洲条约集》第 182 号公约的成员国与《网络犯罪公约》的成员国不同，因此其条款不适用于《网络犯罪公约》所有缔约国之间的合作。谈判第 182 号公约是为了满足欧洲委员会成员国的需要，而不是《网络犯罪公约》所有缔约国的法律要求、制度和需要，尽管原则上，《欧洲刑事事项互助公约》(《欧洲条约集》第 30 号)及其议定书在部长委员会发出邀请后，开放供非欧洲委员会成员国加入。

本议定书的互助条款有一个具体的实质性范围，因为它们适用于“与计算机系统和数据有关的刑事犯罪的具体刑事调查或诉讼，以及收集刑事犯罪的电子形式的证据”(第 2 条)。考虑到这类调查或诉讼的特殊问题——例如数据的不稳定性、与属地和管辖权有关的问题以及请求的数量，第 182 号公约的类似规定可能并非一向以同样的方式适用。

起草者认识到，“由于本公约适用于众多有不同法律制度和文化的缔约国，不可能详细规定每项权力或程序的适用条件和保障”(见《公约》解释性报告第 145 段)。相反，缔约国必须确保“对人权和自由提供充分的保护”，并适用“缔约国必须遵守一些共同标准[和]最低保障”，包括“缔约国根据适用的国际人权文书所承担的义务而产生的……保障”(见《公约》解释性报告第 145 段，见本议定书第 13 条(纳入了《公约》第 15 条))。因此，与第 182 号公约的条款不同(例如关于“通过视频会议进行听证”的第 9 条规定了第 182 号公约缔约国应遵循的具体程序和保障措施)，本议定书的相应规定允许缔约国在执行方面有更大的灵活性。例如，应由缔约国主管机构商定联合调查组的运作程序和条件(见第 12 条第 2 款)，关于视频会议，被请求方在允许通过视频会议听取嫌疑人或被告的陈述时，可要求特别的条件和保障措施(见第 11 条第 8 款)。在本条款规定的范围内，如果缔约国在条件和保障方面的要求未得到满足，缔约国也可决定不予以合作。

186. 本议定书第 11 条和第 12 条仅在没有根据统一或对等立法订立的其他互助条约或安排的情况下适用——除非有关缔约国在其条约或安排不禁止的情况下，相互决定适用任一或全部规定来代替。无论请求方和被请求方之间是否有一项以统一或对等立法为基础的有效互助条约或安排，第 12 条第 7 款均适用。

第 11 条　视频会议

187. 第 11 条主要涉及使用视频会议技术获取证词或陈述。现有的双边和多边互助条约，例如第 182 号公约，可能规定了这种形式的合作。为了不取代专门为满足这些条约或公约缔约国的要求而制定的条款，正如适用于本节的一般原则(第 5 条第 5 款)所述，第 11 条与本议定书的第 12 条一样，“适用于请求方和被请求方之间没有以统一或对等立法为基础的互助条约或安排的情况”。除第 12 条第 7 款另有规定外，第 5 节的规定不适用于存在此种条约或安排的情况。然而，有关缔约国可相互决定适用第 5 节的规定，以代替现有的条约或安排，除非条约或安排的条款禁止这样做。

第 1 款

188. 第 1 款授权通过视频会议向证人或专家获取证词和陈述。本款规定被请求方可自行决定是否接受相互协助请求或规定提供协助的条件。例如，一缔约国可以《公约》第 27 条第 4 至第 5 款规定的理由拒绝或推迟协助。或者，如以其他方式提供协助更为有效，例如以书面形式核证官方或商业纪录，被请求方可选择以这种方式提供协助。

189. 与此同时，预计本议定书缔约国将具备通过视频会议提供协助的基本技术能力。

190. 举行视频会议以获取证词或陈述可能会引起许多问题，其中可能包括法律、后勤和技术问题。为了使视频会议顺利进行，事先的协调是必不可少的。当被请求方提出条件作为举行视频会议的先决条件时，可能需要额外的协调。因此，第 1 款还要求请求方和被请求方在必要时进行协商，以促进解决出现的任何这类问题。例如，正如下文进一步解释的那样，视频会议可能需要遵循某种程序，以便其结果在请求方可以作为证据接受。反之，被请求方可能需要在某些方面适用其自身的法律要求(例如，由证人宣誓或告知其权利)。此外，被请求方可能要求其官员在某些或所有情况下出席视频会议，无论是为了主持流程，还是为了确保作证者或陈述者的权利得到尊重。在这方面，经协商可能会发现，一些被请求方要求其与会官员遇有担心是否符合本国法律的情况时能够干预、中断或停止听证会，而其他缔约国则可能允

许在某些情况下举行没有本国官员参加的视频会议。又如，被请求方可寻求对安全受到威胁的证人、儿童证人及类似证人的特别保障。这类事项需要事先讨论和决定。在某些情况下，被请求方希望采用某种程序，这可能与请求方的法律相冲突，因为这有利于在审判中使用证词或陈述。在这种情况下，双方应尽最大努力，设法找到符合双方需要的创造性解决办法。此外，双方应提前进行协商，以促进问题的解决，例如，如何处理当事人或其法律顾问提出的异议或特权或豁免权主张，或在视频会议期间使用文件或其他证据。此外，由于为举行视频会议而施加的条件，可能需要特定的程序。

还应讨论后勤问题，如请求方是否应为视频会议中己方或被请求方的证词或陈述提供口译和录音，以及启动和维持传输的技术协调，并在传输中断的情况下备有替代的通信渠道。

第 2 款

191. 第 2 款涉及管理这种合作形式的一些程序和相关机制(除本条其余各款规定的其他适用程序和要求外)，这些都是从《公约》中摘录或改编的。第 2 款分为两项。

192. 由于视频会议是一种相互助形式，第 2 款(a)项规定，被请求方和请求方的中央机关应为适用本条的目的相互直接联系。由于本条仅在没有以统一或对等立法为基础的互助协定或安排的情况下适用，这里的“中央机关”是指根据《公约》第 27 条第 2 款(a)项指定的一个或多个机关(见本议定书第 3 条第 2 款(a)项和解释性报告第 38 段)。

193. 本条第 2 款(a)项还规定，被请求方可接受以电子形式进行视频会议的请求，并可在接受请求之前要求适当级别的安全和认证。

194. 第 2 款(b)项(类似于《公约》第 27 条第 7 款)要求被请求方将其不执行或推迟执行请求的理由通知请求方。如上文第 192 段所述，这种沟通应通过中央机关的渠道进行。最后，第 2 款(b)项规定，《公约》第 27 条第 8 款(述及无条约情况下互助请求的保密性)和第 28 条第 2 款至第 4 款(述及无条约情况下答复的保密性和使用限制)适用于视频会议条款。

第 3 款

195. 由于视频会议可能需要请求方的司法官员和辅助人员在跨越很多时区以外的被请求方参与取证或陈述，因此，被听证人在预定时间和地点到场至关重要。根据第 3 款，如果被请求方根据本条提供协助，它必须设法使被要求提供证词或陈述的人到场。如何更好地做到这一点可能取决于案件的情况、被请求方的国内法，以及是否相信此人会在预定时间自愿出庭。相反，为确保此人出庭，被請求方最好发出命令或传票，強制該人出庭，而本款授权被請求方根据其本国法律规定的保障措施这样做。

第 4 款

196. 第 4 款载有举行视频会议的程序。关键目标是以允许在调查和诉讼中作为证据使用的形式向请求方提供证词或陈述。为此，应适用请求方要求的程序，除非这样做不符合被请求方的法律，包括被请求方未编入其立法的适用法律原则。例如，在视频会议期间，首选程序是由被请求方允许请求方当局直接询问被要求提供证词或陈述的人。请求方的检察官、调查法官或调查人员对刑事侦查或起诉最为了解，因此最清楚哪些问题对侦查或起诉最有用，以及如何以符合请求方法律的方式最佳地表述这些问题。在这种情况下，参加审理的被请求方当局只有在必要时才会干预，因为请求方当局的行事方式不符合被请求方的法律。在这种情况下，被请求方可根据其法律和视频会议的情况，不允许提问、接管提问或采取其他适当的行动。“与被请求方的国内法相抵触”一词并不包括程序仅仅与被请求方的程序不同的情况，而这种情况经常会发生。相反，它旨在处理程序与被请求方的法律相悖或不可行的情况。在这种

情形下，或者在请求方没有寻求具体程序的情况下，默认程序将是根据被请求方的法律适用的程序。如果适用被请求方的法律给请求方造成问题，例如在审判中的证词或陈述的可接受性问题，请求方和被请求方可以寻求就不同的程序达成协议，使请求方满意，但又能避免因被请求方法律产生的问题。

第 5 款

197. 第 5 款涉及对虚假陈述、拒绝回答和其他不当行为的惩罚或制裁，其目的是在证人身处与刑事诉讼发生地不同的国家时保护提供证词或陈述过程的完整性。如被请求方已规定此人有义务作证或如实作证，或已禁止此人作出某些行为(例如扰乱诉讼程序)，则该证人须在其所在的司法管辖区承担后果。在这种情况下，被请求方必须能够适用在本国诉讼过程中发生这种行为时应适用的制裁。其适用应不影响请求方的任何管辖权。这一要求进一步鼓励证人作证、如实作证和不从事被禁止的行为。如果被请求方的国内诉讼程序中没有适用的制裁措施(例如对被告的虚假陈述)，则不需要为视频会议期间的此类行为制定任何制裁。这一规定对于确保起诉作假证的证人特别有用，但由于被请求方禁止引渡国民等原因，该证人不能被引渡到请求方接受起诉。

第 6 款

198. 第 6 款规定了关于视频会议过程中产生的费用分摊规则。作为一般规则，视频会议过程中产生的所有费用由被请求方承担，但以下费用除外：(1)专家证人的费用；(2)笔译、口译和笔录费用；(3)数额巨大具有特殊性质的费用。差旅费和在被请求方境内过夜的费用通常不大，因此，如果有这种费用，一般由被请求方承担。然而，关于费用的规则可由请求方和被请求方之间的协议修改。例如，如果请求方提供所需的口译人员在场或在视频会议己方一端提供转录服务，则请求方可能完全没有必要为被请求方提供此类服务付费。如果被请求方根据第 6 款(b)项的规定，预计在提供协助方面会有特殊费用，则请求方和被请求方应在执行请求前进行协商，以确定请求方是否能够承担这些费用，如果不能，则如何避免这些费用。

第 7 款

199. 虽然第 1 款明确授权使用视频会议技术录取证词或陈述，但第 7 款(a)项规定，经双方同意，第 11 条的规定可适用于举行音频会议。此外，第 7 款(b)项规定，经请求方和被请求方商定，技术可用于其他“目的或听证，包括用于识别人或物体”。因此，如果双方同意，请求方和被请求方可考虑使用视频会议技术，以便听取或进行有关嫌疑人或被告人的诉讼(应当指出，有些缔约国可能将嫌疑人或被告人视为“证人”，因此，本条第 1 款已涵盖了对该人证词或陈述的录取)。在第 1 款不适用的情况下，第 7 款规定了允许在这种情况下使用技术的法律依据。

第 8 款

200. 第 8 款涉及被请求方选择允许听取嫌疑人或被告的情况，例如为了提供证词或陈述，或为了通知或其他程序措施。被请求方有权酌情决定是否允许普通证人或专家进行视频会议，同样，被请求方也有权酌情决定是否允许嫌疑人或被告人进行视频会议。此外，除了被请求方为允许进行视频会议可能规定的任何其他条件或限制外，一缔约国的国内法可要求对嫌疑人或被告人的听证规定特殊条件。例如，一缔约国的法律可能要求嫌疑人或被告人同意提供证词或陈述，或者一缔约国的法律可能禁止或限制使用视频会议进行通知或采取其他程序性措施。因此，第 8 款旨在强调，针对嫌疑人或被告人的程序可能会产生对那些本来可能产生的条件或保障加以补充的需要。

第 12 条　联合调查组和联合调查

201. 鉴于网络犯罪和电子证据的跨国性质，与网络犯罪和电子证据有关的调查和起诉往往与其他国家有关联。联合调查组可以成为两个或更多国家之间进行业务合作或协调的有效手段。第 12 条为这种形式的合作奠定了基础。

202. 经验表明，如果一国正在调查与网络犯罪有关的跨境犯罪，或需要获得电子证据，此种调查也可以从正在调查相同或相关行为的其他国家当局的参与受益，或其他方面的协调是有益的。

203. 如本议定书第 5 条和解释性报告第 182 至 186 段所述，第 12 条的规定不适用于请求方和被请求方之间存在有效的以统一或对等立法为基础的互助条约或安排，除非有关缔约国共同决定，在条约或安排不禁止的情况下，适用本条的任一或全部其余内容来代替。如下所述，无论请求方和被请求方之间是否有一项以统一或对等立法为基础的有效互助条约或安排，第 7 款均适用。

第 1 款

204. 第 1 款规定，两个或多个当事方的主管机构可在其认为特别有用的情况下商定设立联合调查组。联合调查组是通过双方协议达成的。第 12 条中使用的“相互协议”、“协定”和“同意”等词不应理解为要求有国际法规定的有约束力的协定。

205. 本条使用了两个相关术语：“主管机构”和“参与机构”。由每个缔约国决定哪些机构有资格——即“主管机构”——签订联合调查组协议。一些缔约国可授权一系列官员，如检察官、调查法官或指挥刑事调查或诉讼的其他高级执法官员签订此种协议；其他缔约国则可能要求中央机关——通常为负责互助事务的办事室——这样做。关于哪些机构实际参加联合调查组的决定——“参与机构”——同样将由各缔约国决定。

第 2 款

206. 第 2 款规定了联合调查组运作的程序和条件，例如其具体目的、组成、职能、期限和任何延长期、地点、组织、收集、传递和使用信息或证据的条件，保密要求一方的参加机构参与在另一方领土上进行的调查活动的条件，应由这些主管机构商定。特别是，在拟定协议时，有关缔约国不妨讨论拒绝或限制使用信息或证据的条件，包括，例如，根据《公约》第 27 条第 4 或第 5 款规定的理由，以及如果需要信息或证据用于所签协议以外的目的(包括控方或辩方在另一案件中使用该信息或证据，或可能需要防止第 3 条第 2 款界定的紧急情况，即任何自然人的生命或安全面临重大、迫在眉睫的危险的情况)则应遵循何种程序。鼓励缔约国在协议中明确规定对实际在另一缔约国境内的该方的参与官员的权力限制。还鼓励缔约国在协议中允许以电子方式传送所收集的信息或证据。

207. 预计双方通常将以书面形式共同确定这些程序和条件。在任何协议中，都应考虑到所需的详尽程度。精简文本可以为可预见的情况提供必要的精准程度，如果未来的情况需要进一步的精准，还可以增加补充条款。双方应考虑联合调查组协议的地理范围和持续时间，以及随着新情况的出现，协议可能需要修改或扩大的情况。

208. 作为联合调查组一部分使用的信息或证据可能包括用户信息、流量数据或内容数据等形式的个人数据。与本议定书下的其他合作措施一样，第 14 条适用于根据联合调查组的要求转交个人数据。

209. 如同一缔约国根据本议定书收到的所有资料或证据的一般情况一样，该缔约国适用的证据规则将决定该资料或证据在司法程序中是否可予采纳。

第 3 款

210. 第 3 款允许缔约国在签署本议定书时，或交存批准书、接受书或核准书时，声明其中央机关必须是设立工作组协议的签署方或同意方。加入这一条款有几个原因。首先，一些缔约国认为，联合调查组是一种互助形式，在其他一些缔约国，当主管机关(可能是检察官或警察，其国际合作经验相对有限)根据本条准备联合调查组协议时，负责互助的中央机关可能在确保适用的国内法律要求得到满足方面发挥作用。中央机关在关于互助和其他形式国际合作的国际协议(包括本议定书)方面的经验，也可有助于其在确保满足本议定书的要求方面发挥重要作用。最后，如果一个缔约国作出了该款规定的声明，其他缔约国当局如果想与作出声明的缔约国达成联合调查组协议，就会注意到作出声明的缔约国的中央机关必须签署或以其他方式同意联合调查组协议，以便根据本议定书使之有效。这就防止了在没有必要的授权或不符合声明方适用的法律要求的情况下订立联合调查组协议。

第 4 款

211. 根据第 4 款，缔约国根据第 1 款确定的主管机关和第 2 款所述的参与机构通常将直接相互沟通，以确保效率和效果。然而，如果在特殊情况下可能需要更多的中央协调——如影响特别严重的案件或引起特别协调问题的情况——则可商定其他适当的渠道。例如，中央互助机关可协助协调这类事宜。

第 5 款

212. 第 5 款规定，如果需要在当事一方的领土上采取调查措施，该方的参与机构可以要求本身的主管机构采取这些措施。这些官方机构根据国内法确定是否可以采取调查措施。如果它们能够这样做，则无需其他缔约国提出互助请求。这提供了联合调查组最具创新的方面之一。然而，在某些情况下，这些官方机构可能没有足够的国内权力代表另一缔约国在未提出互助请求的情况下采取特定的调查措施。

第 6 款

213. 第 6 款述及一缔约国参与机构使用从另一缔约国参与机构获得的信息或证据的问题。可根据第 1 款和第 2 款所述协议的条款拒绝或限制使用；但是，如果该协议未规定拒绝或限制使用的条款，则可按第 6 款(a)至(c)项规定的方式使用该信息或证据。第 6 款所述情况不妨碍第 14 条对向另一国转交信息或证据所规定的要求。

214. 应当指出的是，在适用第 6 款(a)至(c)项的情况下，参与机构仍可相互决定进一步限制使用特定信息或证据，以避免在提供信息或证据之前，特别是之后，对其调查造成不利后果。例如，即使证据的使用是为了收到证据的缔约国建立联合调查组的目的，也可能对提供信息或证据的缔约国的调查产生不利影响(例如向犯罪集团泄露在进行调查，因而可能造成犯罪分子逃跑、销毁证据或恐吓证人)。在这种情况下，提供信息或证据的一方可要求另一方同意，在该风险消除之前不公开该信息或证据。

215. 在第 6 款(b)中，起草人打算在协议没有规定拒绝或限制使用条件的情况下，如果根据参与机构收到信息或证据的一方的基本法律原则，对于在事关其他此类罪行的诉讼中进行有效辩护至关重要的信息或证据，必须向辩护方或司法机关披露，则不需要提供信息或证据的官方同意。即使在这种情况下不需要征得同意，也应通知披露为此目的提供的信息或证据，不得无故拖延。如有可能，应在披露之前发出此类通知，以使提供信息或证据的一方能够为披露做好准备，并允许双方酌情进行协商。

216. 起草者的理解是，第 6 款(c)项是指接收方官方可以直接使用该信息或证据来防止本议定书第 3 条第 2 款(c)项所界定的紧急情况的特殊情形。自然人的安全意味着严重的身体伤害。本解释性报告第 42 段较详细地解释了“任何自然人的生命或安全面临重大、迫在眉睫的危险”

的概念，并提供了这类情况的例子。起草者认为，对资产或网络的重大、迫在眉睫的威胁涉及自然人的生命或安全的情况应包括在这一概念中。如果根据第 6 款(c)项使用了信息或证据，除非双方另有决定，否则应立即通知提供信息或证据的一方的参与机构。例如，参与机构可确定应否通知其中央机关。

第 7 款

217. 最后，应总地回顾，执法伙伴之间临时开展国际合作努力由来已久，其中一个国家的检察官和(或)调查员小组与外国同行合作开展特定调查，而不是在联合调查组的基础上开展合作。第 7 款规定了这类国际合作努力，并为在没有第 1 款和第 2 款所述协议的情况下进行联合调查提供了条约依据(若一缔约国要求此种法律依据的话)。如下所述，无论请求方和被请求方之间是否有一项以统一或对等立法为基础的有效互助条约或安排，第 7 款均适用。与本议定书规定的所有措施一样，第 7 款规定的联合调查须遵守第三章的条件和保障措施。

第三章　条件和保障

第 13 条　条件和保障

218. 依照《公约》第 15 条，第 13 条规定，“各缔约国应确保本议定书规定的权力和程序的确立、实施和应用符合其国内法律规定的条件和保障，这些条件和保障应充分保护人权和自由”。由于本条以《公约》第 15 条为基础，《公约》解释性报告第 145 至 148 段中对该条的解释对本议定书第 13 条也有效，包括相称性原则，“各缔约国根据其国内法的相关原则执行相称性原则”(见《公约》解释性报告第 146 段)。

219. 应当指出，除本条外，其他条款也载有重要的保障措施。例如，本议定书的措施范围有限，即“适用于与计算机系统和数据有关的刑事犯罪的具体刑事调查或诉讼，以及收集刑事犯罪的电子形式的证据”(见第 2 条)。此外，个别条款规定了请求、命令和可能有助于适用国内保障措施的附带信息((见第 6 条第 3 款，第 7 条第 3 和第 4，第 8 条第 3 款，第 9 条第 3 款)。此外，在每一条款中规定了要披露的数据类型，例如，第 7 条仅限于用户信息。另外，缔约国可以作出保留和声明，例如限制所提供的信息类型，如第 7 条和第 8 条。最后，在根据本议定书转交个人数据时，适用第 14 条的数据保护保障。

第 14 条　保护个人数据

第 1 款 范围

220. 本议定书第二章规定的措施往往涉及个人数据的传输。鉴于本议定书的许多缔约国为了履行其宪法或国际义务，可能需要确保对个人数据的保护，第14条规定了数据保护的保障措施，使缔约国能够满足这些要求，从而能够为本议定书的目的处理个人数据。

221. 根据第 1 款(a)项，各缔约国应按照本条第 2 款至第 15 款的规定处理其根据本议定书收到的个人数据。这包括根据本协议作为命令或请求的一部分传输的个人数据。但是，如果第 1 款(b)项或第 1 款 c)项所述的例外条款适用，则第 2 款至第 15 款不适用。

222. 第一个例外载于第 1 款(b)项，其中规定，“如果在根据本议定书收到个人数据时，转交方和接收方都受一项国际协议的约束，该协议在双方之间确立了一个保护个人数据的全面框架，适用于为预防、侦查、调查和起诉刑事犯罪目的转让个人数据，其中规定，根据该协议处理个人数据符合有关缔约国数据保护立法的要求，则该协议的条款，作为属于该协议范围的措

施，应适用于根据本议定书收到的个人数据，以代替第 2 款至第 15 款，除非当事各方另有约定”。在这种情况下，如果一个框架全面涵盖了数据传输的数据保护方面，则该框架通常被视为是“全面的”。第 1 款(c)项所述协定的两个例子是经《欧洲委员会条约集》第 223 号议定书修正的《在个人数据自动处理方面保护个人的公约》(《欧洲条约集》第 108 号)，以及《美利坚合众国和欧洲联盟关于保护与预防、调查、侦查和起诉刑事犯罪有关的个人信息的协定》。此类协定的条款应代替第 2 款至第 15 款适用于属于此类协定范围的措施。对于经《欧洲委员会条约集》第 223 号议定书修正的《欧洲条约集》第 108 号公约的缔约国，这意味着该条约第 14 条第 1 款适用，本解释性报告第 105 至 107 段对此作了进一步解释。就时间而言，只有双方在根据本议定书收到个人数据时相互受协议约束的情况下，本条第 2 款至第 15 款才可被取代。只要协议规定根据其传输的数据继续根据该协议的条款进行处理，这一点就适用。

223. 第二种例外情况载于第 1 款(c)项，该款规定，如果转交方和接收方不受第 1 款(b)项所述协议的约束，二者可以共同决定，根据本议定书转交个人数据可以基于当事方之间的其他协议或安排进行，以取代第 2 款至第 15 款。这确保了缔约国在决定适用于彼此间根据本议定书转交的数据保护的保障方面保持灵活性。为了给个人和根据本议定书第二章第 2 节的措施参与数据转交的供应商和实体提供法律方面的确定性和透明度，鼓励缔约国向公众明确传达其共同决定，即此类协议或安排适用于缔约国之间个人数据传输的数据保护方面。

224. 起草者认为，通过本条第 2 至第 15 款规定的数据保护保障，本议定书确保对本议定书下的数据转交提供恰当的保护。为此，根据第 1 款(d)项，第 1 款(a)项规定的数据转交应被视为符合各缔约国个人数据国际转交的数据保护法律框架的要求，而且根据这些法律框架，这种转交不需要进一步授权。

此外，只要第 1 款(b)项所述的协议在自身条款中规定，根据这些协议对个人数据的处理符合有关缔约国的数据保护法要求，第 1 款(d)项就将这种认可扩大到本议定书下的转交。因此，本款为根据第 1 款(a)项或第 1 款(b)项应本议定书下的命令和请求进行的个人数据国际转交提供了法律确定性，以确保有效和可预测的数据交换。由于第 1 款(c)项所述的协议或安排可能并非始终提及遵守缔约国关于国际转交的数据保护法律框架——例如在双边互助条约的情况下——它们在本议定书中没有得到与第 1 款(a)项或第 1 款(b)项相同的认可。但是，有关缔约国可通过共同决定作出这种认可的规定。

225. 此外，第 1 款(d)项规定，缔约国只能以数据保护为由拒绝或阻止根据本议定书向另一缔约国转交个人数据：(1)在第 1 款(a)项适用的情况下，根据第 15 款规定的关于协商和中止的条件，或(2)在第 1 款(b)项或(c)项适用的情况下，根据这两款中的一款所提及的具体协议或安排的规定。

226. 最后，第 14 条的目的是确立适当的保障，允许缔约国之间根据本议定书转交个人数据。第 14 条并不要求统一处理个人数据的一般国内法律框架，也不要求统一具体为执行刑法而处理个人数据的框架。第 1 款(e)项规定，不排除缔约国对其本国官方处理根据本议定书收到的个人数据时，适用比第 2 至 15 款规定的更有力的数据保护保障。反之，第 1 款(e)项的目的是，不允许缔约国对本议定书下的数据转交施加超出该条允许的具体额外数据保护要求。

第 2 款 目的和用途

227. 第 2 款述及缔约国可根据本议定书处理个人数据的目的和用途。第 2 款(a)项规定，“收到个人数据的缔约国应按第 2 条所述的目的处理这些数据”，即为“与计算机系统和数据有关的刑事犯罪的特定刑事调查或诉讼”和“收集刑事犯罪的电子形式证据”的目的，在《第一项议定书》缔约国之间，为“对根据《第一项议定书》确立的刑事犯罪进行具体的刑事调查或

诉讼”的目的。换句话说，官方必须调查或起诉特定的犯罪活动，这是可以寻求和处理包含个人数据在内的证据或信息的合法目的。

228. 虽然在第一种情况下，只有为了在具体的刑事调查或诉讼中获得信息或证据，而不是为了其他目的，才能援引本议定书，但第 2 款(a)项还规定，缔约国“不得出于不相符合的目的进一步处理个人数据，也不得在其国内法律框架不允许的情况下进一步处理这些数据”。在确定进一步处理的目的是否与最初的目的相抵触时，鼓励主管机构对具体情况进行全面评估，例如：(1)最初的目的和进一步的目的之间的关系(例如任何客观联系)；(2)考虑到个人数据的性质(例如其敏感性)，预期进一步使用对相关个人的(潜在)后果；(3)有关个人对进一步使用目的以及哪些实体可能处理数据的任何合理预期；以及(4)处理数据和防止不当使用数据的方式。缔约国的法律框架可进一步规定关于数据可能用于的其他目的的具体限制。

229. 为了互不抵触的目的进行处理，通常包括根据刑法领域的国内法和国际协议或安排(例如互助)将数据用于国际合作。除其他外，它还可包括用于某些政府职能，如向监督机构报告；对违反刑法、民法或行政法的行为进行相关调查(包括其他政府部门进行的调查)及其裁决；国内法院命令所要求的披露；向私人诉讼当事人披露；向被告的律师透露某些信息；以及直接向公众或新闻媒体披露(包括在查阅文件请求和公共法律程序的情况下)。同样，为公众利益、科学或历史研究或统计目的存档进一步处理个人数据也可视为符合规定。

230. 第 2 款(a)项还允许缔约国在本议定书第二章规定的范围内，对个人数据的使用施加额外的条件和限制。但是，此类条件不应包括第 14 条规定的条件以外的通用数据保护条件，即不针对具体案例的条件。例如，根据第 14 款，接受不同的监督制度，一方不得将请求方拥有相当于专门的数据保护机构作为个别情况下的转交条件。

231. 最后，第 2 款(b)项要求，在根据本议定书寻求和使用个人数据时，“接收方应根据其国内法律框架确保所寻求和处理的个人数据与此类处理的目的相关，且不过度”。这一要求可以通过证据规则和对强制命令的范围的限制、必要性和相称性原则、合理性原则以及限制数据收集或使用的内部准则和政策等来实施。还鼓励缔约国在其国内法律框架下，审议涉及受害者或未成年人等弱势个人的情况。

第 3 款 质量和完整性

232. 第 3 款要求各缔约国“应采取合理步骤，确保个人数据的准确性和完整性，并在考虑到处理个人数据目的的情况下，为其合法处理保持所必需和适当的更新”。背景很重要，因此这一原则可以根据不同的情况以不同的方式实施。例如，该原则对刑事诉讼的适用不同于对其他目的的适用。

233. 关于刑事调查和诉讼，第 3 款不应被视为要求刑事执法机构改变可能构成刑事案件证据的信息——即使这些信息不准确或不完整，因为数据的不准确可能是犯罪的核心(例如在欺诈案件中)，而且如果当局修改通过本议定书收集的证据，也会损害公平对待被告的目标。

234. 在许多情况下，当对个人数据的可靠性持有疑问时，应明确指出这一点。例如，如果通过本议定书收到的信息或证据被用于追踪过去的犯罪行为，适用的程序应提供纠正或记录信息中错误的手段(例如通过修改或补充原始信息)，以及用于更新、修改或补充不可靠或过时的数据，以最大限度地减少官方因数据质量差而采取不适当和可能不利的执法行动的风险(例如，逮捕错误的人或按照对某人行为的错误理解而逮捕此人)。鼓励各缔约国采取合理步骤，确保在发现向另一官方机构提供的或从另一官方机构收到的数据不正确或过时之时，尽快通知该官方机构，以便根据处理的目的，在必要和适当的范围内作出更正。

第 4 款 敏感数据

235. 第 4 款涉及缔约国在处理某些类型的数据时应根据本议定书采取的措施，这些数据可能是刑事调查或诉讼中特别需要作为证据的数据，但同时其性质需要适当的保障措施，以防止使用这类数据对有关个人造成不必要的不利影响，特别是防止非法歧视。

236. 第 4 款规定，敏感数据包括“可披露种族或族裔血统、政治观点或宗教或其他信仰、或工会成员身份的个人数据、遗传数据、生物特征数据(鉴于所涉风险被视为敏感数据)、或有关健康或性生活的个人数据”，其中包括性取向和性行为。健康数据可包括与个人的身体或精神健康相关的数据，这些数据揭示此人过去、现在或将来健康状态的信息(例如，关于疾病、残疾、疾病风险、个人病史或治疗状况、或个人的生理或生物医学状态的信息)。遗传数据可包括例如由染色体、脱氧核糖核酸(DNA)或核糖核酸(RNA)分析产生的数据，并且涉及人的遗传或后天遗传特征，该遗传特征包含关于此人的生理、健康或亲子关系的独特信息。

237. 生物特征数据的概念涵盖了一系列独特的标识，这些标识是由可测量的身体或生理特征产生的，用于识别或核实个人声称的身份(例如指纹、虹膜或手掌静脉图形、声音模式、照片或录像)。一些缔约国还认为，生物或行为特征所产生的独特识别标志构成生物特征数据。鉴于所涉及的风险，某些形式的生物特征数据可能被认为是敏感的，而其他形式可能不是。例如，一些缔约国认为，从生物特征样本或图像(如生物特征模板)中计算或提取的生物特征数据是敏感的。相反，某些照片或录像片段，即使它们显示了身体或解剖特征，如疤痕、皮肤印记和纹身，一般也不被视为属于敏感的生物识别数据的范畴。由于生物测定数据的敏感程度可能不同，第 4 款为缔约国提供了监管这一领域的灵活性，指出敏感数据包括“鉴于所涉风险被视为敏感数据”，从而为缔约国管理这一领域提供了灵活性。该措辞承认生物识别技术是一个不断发展的领域，根据本款被视为“敏感”的数据，需要随着时间的推移，结合技术、调查和其他发展以及对所涉个人的风险进行评估。关于经《欧洲委员会条约集》第 223 号议定书修正的《关于在自动处理个人数据方面保护个人的公约》(《欧洲条约集》第108 号)的缔约国，对于什么是“敏感”生物识别数据的解释，应以该条约第 6 条第 1 款为指导，其该条约解释性报告第 58 和 59 段对此作了进一步详述。

238. 滥用和不当处理敏感数据可能会对个人造成无端偏见，包括非法歧视。刑事司法系统的结构应能防范无端偏见和非法歧视的影响，例如，缘于使用披露种族、宗教或性生活的证据。另一个例子是，该款还承认，必须防范因不正当或非法披露而造成伤害的风险，例如，一个人因性取向或性别认同的信息被披露而受到排斥。在这方面，第 4 款要求缔约国提供“适当的保障措施”，以防范这种风险。

239. 评估保障措施是否适当，应参考数据的敏感性和处理的范围、背景、目的和性质(例如在自动决策的情况下)，以及风险的可能性和严重程度。这些保障措施可能因国内法律制度而异，并取决于这些因素。一份非详尽的保障措施清单可能包括限制处理(例如，仅允许为某些目的或在个案基础上进行处理)、限制传播、限制访问(例如，通过特别授权或认证程序限制某些人员访问，要求对这些人员进行专门培训)、额外的组织或技术安全措施(例如，屏蔽、使用假名或将生物识别数据的存储与相关生物信息分开)或缩短保留期。在某些情况下，作出影响评估可能有助于识别和管理风险。

第 5 款 保留期限

240. 第 5 款第一句规定，“各缔约国应仅限于第 2 款处理数据的目的，在必要和适当的时间范围内保留个人数据”。在这方面，第 2 款的目的限制原则规定，收到个人数据的缔约国应根据第 2 条为特定目的处理数据，不得为不相容的目的进一步处理数据。根据这一原则，数据保留期限与处理数据的特定目的相关。

241. 由于根据第 2 条，缔约国根据本议定书收到的个人数据是为了具体的刑事调查或诉讼程序，只要有需要就可以保留个人数据：(1)在调查和随后的诉讼期间，包括任何上诉或根据国内

法律可能重新审理案件的期间；(2)在最初收集的目的完成后，为与最初目的“不相抵触”的目的作进一步处理。例如，一缔约国可规定，按照第 14 条第 2 款的规定，为存档或历史研究目的或其他兼容目的保存信息或证据，本解释性报告相应段落对此作了进一步解释。

242. 第 5 款第二句为缔约国提供了两种选择，以履行保留个人数据的义务，即根据本条第 2 款处理数据的目的，只保留必要和适当的时间。首先，缔约国可在其国内法律框架中规定具体的保留期限。或者，缔约国可在其国内法律框架中规定，在计划的间隔期内，审查进一步保留的必要性。缔约国有一定的自由裁量权，可在其国内法律框架内，决定哪种方法最适合具体的数据集。缔约国也可将具体的保留期与间隔时间较短的定期审评制度结合起来。缔约国应在其法律框架内确保主管机构制定内部规则和(或)程序，以执行具体的保留期和(或)定期审查进一步保留的必要性。如果保存期已过，或缔约国通过定期审查确定不再需要保存数据，则应删除数据或使之匿名。

第 6 款 自动决定

243. 第 6 款涉及在对个人相关利益产生重大不利影响的决定完全基于对其个人数据的自动处理时对个人的保护。当一缔约国根据本议定书从另一缔约国收到个人数据时，预计不会经常涉及自动决定，因为调查人员或司法当局将为具体刑事调查或诉讼收集证据或信息。然而，如果自动决定对与个人数据有关的个人的相关利益产生重大不利影响，而在调查中又要求提供这些数据，则当局必须遵守这一规定。如果随后将数据用于预防、侦查、调查或起诉其他犯罪(例如，基于对犯罪特征纯粹自动化处理的逮捕、判刑、保释、假释)，或用于兼容目的(例如，背景调查)，如果为决策目的对数据使用自动化分析工具，当局也必须遵守这一规定。

244. 因此，第 6 款禁止仅仅根据对个人数据的自动处理，作出对个人相关利益产生重大不利影响的决定，包括不利的法律影响(通过影响个人的法律地位或权利)，如发出逮捕令或拒绝保释或假释，除非这种决定是根据国内法授权作出的，并受适当保障措施的制约。

245. 适当的保障措施对于减少对个人数据所涉个人的相关利益产生潜在影响至关重要。这种保障措施应包括当事人获得人为干预以评估决定的可能性。还鼓励缔约国采取合理步骤，确保用于制定算法的数据的质量和代表性，以及所使用的统计推断的准确性，同时考虑到具体的处理情况和背景，包括刑事执法的背景。

第 7 款 数据安全和安全事件

246. 根据第7款(a)项，“各缔约国应确保采取适当的技术、物理和组织措施以保护个人数据”。例如，技术措施可包括软件保护，防止计算机恶意软件、数据加密和防火墙。物理措施可包括将计算机服务器和文件存储在安全位置，组织措施可包括规则、实践、政策和程序，包括限制访问权限等措施。

247. 第 7 款(a)项还规定，这些措施尤其必须防范损失(例如归档和处理数据的标准化程序)、意外或未经授权的访问(例如防止计算机入侵、访问纸质文件或计算机文件的授权或认证要求)、意外或未经授权的披露(例如，检测和防止意外或未经授权披露的技术措施，以及概述此类披露后果的组织措施)，以及意外或未经授权的数据更改或销毁(例如，限制授权人员输入或更改电子数据或纸质文件、使用记录系统、显示保存期限、安装计算机或纸质文件备份系统)。

248. 以适合具体情况的方式满足这些要求的确切方式由有关缔约国决定。例如，鼓励缔约国设计和实施安全措施，其中考虑到个人数据的性质(包括其敏感性)、已确定的风险以及在发生安全事件时对有关个人的任何潜在不利后果等因素。同时，缔约国可考虑到设计和执行数据安

全措施所涉资源问题。鼓励缔约国定期审查此类措施，并根据技术的发展和风险性质的变化酌情更新这些措施。

249. 第 7 款(b)项规定了在发生与根据本议定书收到的个人数据有关的“安全事件”(定义见第 7 款(a)项和上文所述)时，对个人或数据来源方造成“重大人身或非人身伤害风险”的要求。对个人的相关伤害可能包括，例如身体或名誉伤害、精神痛苦(例如通过羞辱或违反保密规定)、歧视或经济伤害(例如丧失就业或职业机会、负面信用评级、身份被盗或可能被勒索)。对另一方而言，相关损害尤其可能包括对平行调查的潜在负面影响(例如嫌疑人潜逃、销毁证据)。如果存在这种损害的“重大危险”，接受方有义务“立即评估损害的可能性和规模，”并“应迅速采取适当行动减轻此类损害”。除其他外，应考虑的与损害的可能性和规模有关的因素，可包括事件的类型，例如，如果知道，它是否是恶意的；拥有或能够获得该信息的人；受影响数据的性质和敏感性；可能受到危害的数据量和可能受影响的个人数量；识别相关人员的难易程度；访问和使用数据的可能性，例如数据是否被加密或以其他方式使其无法访问；以及作为事件的结果可能发生的可能后果。

250. 根据第 7 款(a)项所述的措施，并为确保第 7 款(b)项所述的适当应对措施，缔约国必须建立内部程序，以便能够发现安全事件。缔约国还应制定一个流程，用于迅速评估潜在损害的可能性和规模，并迅速采取适当措施，减轻损害(例如，通过召回或请求删除意外传输给未经授权接收者的信息)。内部报告程序和保存任何安全事件的记录可使这些要求得到有效应用。

251. 第 7 款(b)项还规定了在哪些情况下必须将事件通知另一方和受影响的个人，但有例外和限制。

252. 如果发生对个人或另一方造成重大人身或非人身伤害风险的安全事件，应通知转交当局，或为第二章第 2 节的目的，通知根据第 7 款(c)项指定的一个或多个机构。但是，通知可以包括对进一步传送通知的适当限制，在这种通知可能危及国家安全时，可以推迟或不作通知，或者当这种通知可能危及保护公共安全的措施时(包括在通知可能危及对安全事件引起的刑事犯罪的调查时)可以推迟。在决定是否应在通知可能危及国家安全的情况下延迟或不通知时，缔约国应考虑在这种情况下不通知是否合理，或延迟通知是否更为恰当。

253. 如果发生对个人造成重大人身或非人身伤害风险的安全事件，还应向受该事件影响的个人发出通知，使他们能够保护自己的利益，但也有例外情况。第一，第 7 款(b)项规定，如果缔约国已采取适当措施，不再有重大损害危险，则不必发出通知。例如，如果包含敏感个人信息的电子邮件意外发送给错误的收件人，如果不采取措施减轻影响，将造成重大损害风险，但在进一步共享之前，收件人根据请求迅速永久删除了该邮件，则无需通知。第二，根据第 12 款(a)项(1)目规定的条件，可推迟或不通知有关个人，即通知“恪守其国内法律框架允许的适当限制……为保护他人的权利和自由或一般公共利益的重要目标所需要且适当考虑到有关个人合法利益”。

254. 一般而言，鼓励缔约国在根据第 7 款(b)项发出的通知中，酌情列入关于安全事件的类型、可能受到损害的信息的类型和数量、可能的风险以及为减轻可能的损害而设想采取的措施，包括遏制事件的措施。鉴于其监督职能，并为了在处理事件方面受益于专家的咨询意见，通知方还宜向第 14 款所述监督机构通报事件和任何缓解措施。

255. 为了协调响应并支持其自身的风险缓解工作，被通知方可要求通知方协商和提供有关事件及其响应的补充信息。

256. 第 7 款(c)项规定了缔约国为第二章第 2 节的目的，指定应根据第 7 款(b)项通知的一个或多个主管机构所需的程序。

第 8 款 保存记录

257. 第 8 款要求缔约国“保存记录或采用其他适当手段，证明在特定情况下如何获取、使用和披露个人数据”。其目的是让每个缔约国拥有有效的手段来证明特定个人的数据是如何根据本条规定在特定情况下获取、使用和披露的。表明遵守情况对于监督目的尤其重要，因此有助于问责。虽然表明如何处理数据的确切方法由各缔约国自行实施，但鼓励各缔约国根据具体情况调整方法，同时考虑到对有关个人的风险以及处理的性质、范围、目的和总体背景。

258. 例如，一些缔约国可能决定利用活动的自动记录(日志记录)或其他替代办法(如遇有纸质档案的情况采用手写记录)。如上所述，目标是促进问责制，但在缔约国如何这样做的方面允许一定程度的灵活性，以符合第 14 条下的其他适用义务。例如，缔约国应以方便监督机构工作的方式保存关于查阅、使用或披露的记录或其他文件。

第 9 款 缔约国内部的后续共享

259. 第 9 款规定，“当一缔约国的某一主管机构向该缔约国的另一主管机构提供最初根据本议定书收到的个人数据时，该另一主管机构应根据本条处理该数据，但须遵守第 9 款(b)项的规定”。换句话说，如果根据本议定书收到的个人数据随后提供给同一缔约国的另一机构----包括提供给另一个组成州或类似的领土实体的官方机构----则必须根据本条处理此类数据，除非第 9 款(b)项的例外情况适用。第 9 款也适用于多次后续分享的情况。

260. 第 9 款(b)项规定了第 9 款(a)项的一个例外，即一个联邦国家缔约国根据第 17 条规定的条件，对本议定书的义务提出保留。根据本解释性报告第 297 段，这一例外照顾到“联邦国家由于中央和地方当局之间权力分配的特点可能面临的困难”。另见《公约》解释性报告第 316 段。因此，第 9 款(b)项指出，如果一个缔约国根据第 17 条作了保留，它仍然可以将最初根据本议定书收到的个人数据提供给其组成州或其他类似的领土实体，条件是该缔约国已采取措施，以便接收机构继续有效地保护数据，为数据提供与本条规定相当的保护水平。一缔约国未能“采取措施，以便接收的主管机构继续有效地保护数据，为数据提供与本条规定水平相当的保护”，视其未能满足这一要求的严重程度、理由和情节而定，可能构成第14条第 15 款所述的重大或系统性违约。

261. 第 9 款(c)项规定，如有迹象表明另一缔约国对本款实施不当，转交方可要求与该另一缔约国进行协商，并要求提供关于这些迹象的相关信息，以澄清事实。

第 10 款 继而转交给另一个国家或国际组织

262. 根据第 10 款(a)项，对于根据本议定书收到的个人数据，缔约国“只有在获得转交方机构的事先授权，或就第二章第 2 节而言，获得根据第 10 款(b)项指定的一个或多个主管机构的事先授权，方可将个人数据转交给另一个国家或国际组织”。这类保护措施是在刑事执法背景下协助外国合作伙伴的一种常见转移条件(例如根据互助条约或警方与警方的合作)，这一做法也作为保护根据本议定书转交的个人数据的一种手段延续至本款。

263. 第 10 款(b)项规定，各缔约国在签署本议定书时，或交存批准书、接受书或核准书时，应向欧洲委员会秘书长通报为第二章第 2 节的目的提供授权的一个或多个主管机构；所提供的信息而后可以修改。

264. 获得继续传输的授权可能需要接收方机构向传输方机构发送单个请求，以获得授权将具体确定的个人数据传输到特定的第三国或国际组织。然而，第 10 款(a)项并不阻止缔约国事先规定后续传输的规则(例如通过书面协议或其他安排)。第 10 款(a)项也不影响缔约国根据第二

章的具体规定，对数据接收方的使用施加其他条件的能力(例如，对接收方使用或传播个人数据的程度施加限制，以避免妨碍转交方的调查)。

265. 在确定是否根据第10款授权进行转交时，鼓励转交机构或指定机构适当考虑所有相关因素，包括刑事犯罪的严重性、数据最初转交的目的、与最初转交有关的任何适用条件，以及第三国或国际组织是否确保对个人数据的适当保护水平。

第 11 款 透明度和通知

266. 第 11 款(a)项就第 11 款(a)项(1)至(4)目所述事项，对缔约国提出了涉及透明度和通知的某些要求。这些透明度和通知要求有助于个人了解缔约国可能如何处理其数据。这些要求还向个人通报了可用的查阅、纠正和补救措施。

267. 各缔约国可灵活决定，是通过向公众发布一般通知(例如在政府网站上发布)，还是通过向其个人数据已被该方接收的个人发布个人通知的方式，提供此类通知和透明度。通知应易于获取和理解。无论是提供一般通知还是个人通知，都必须包括以下信息：(1)数据处理的法律依据和目的，包括预期或通常披露的目的；(2)根据第 5 款规定的任何保留期或审查期(视情况而定)；(3)向其披露此类数据的接收者或接收者类别；(4)可供查阅、纠正以及司法和非司法补救方式。

268. 根据第 11 款(b)项，当向缔约国已收到数据的个人提供个人通知时，第 11 款(a)项的通知和透明度要求可根据本条第 12 款(a)项(1)目规定的条件受到合理的限制。例如，在刑事司法事项中，可能存在延迟或不提供通知的合法情形。第 12 款(a)项(1)目提到了这类情况，本解释性报告第 272 段对这类情况作了说明。根据信息的敏感性，还可能出现一般通知中提供的细节数量可能受到限制。

269. 第 11 款(c)项为缔约国在刑事司法事项中兼顾透明度好处和保密需要奠定了基础。它规定，如果转交方的国内法律框架要求向根据本议定书向另一缔约国提供其个人数据的人发出通知，转交方应采取措施，在转交时将这一要求和适当的联系方式通知接收方。在第12款(a)项(1)目所述限制条件适用的情况下，如果接收方要求对提供数据加以保密，则转交方不得向个人发出通知。一旦这种限制条件不再适用，并且可以提供个人通知，接收方应采取措施，以便通知转交方可以发出通知。这可能包括定期审查是否需要这种限制。如果转交方尚未收到通知，则转交方有权向接收方提出要求，接收方应通知转交方是否维持限制。

第 12 款 查阅和纠正

270. 第 12 款(a)项要求各缔约国，应确保根据本议定书个人数据为他方收到的任何个人，有权按照国内法律框架规定的程序，寻求和获得查阅此类数据的机会，不得无故拖延(但须受可能的限制)，并在无不当延误的情况下，寻求并获得纠正。“按照国内法律框架规定的程序”一语使缔约国在如何寻求和获得查阅和纠正方面具有灵活性，其意指适用的法律、法规、规则(如管辖规则)和政策以及适用的证据规则等中确立的程序。在一些法律制度中，个人在寻求司法补救之前，需要通过行政手段作出查阅和纠正。

271. 第 12 款(a)项(1)目规定，在提出查阅请求的情况下，个人有权以书面或电子形式保存涉及本人并含其个人数据的文件的副本，表明数据处理的法律依据和目的、保留期限和数据接收者或接收者类别的现有信息(“查阅”)，以及关于根据第 13 款可采取的补救措施的信息。这也可使个人确认其个人数据是否已根据本议定书收到，以及是否已经或正在处理。提供包含可用信息的文件，说明处理的法律依据和目的，将有助于个人评估个人数据是否根据适用法律进行了处理。许多缔约国可能已经通过隐私权、信息自由或政府记录查阅法为这种查阅提供了框架。

272. 在特定案件中获得这种查阅能力可能受到缔约国国内法律框架所允许的适当限制，“在裁决时为保护他人的权利和自由或一般公共利益的重要目标所需要且适当考虑到有关个人合法利益”。例如，他人的权利和自由可能包括其他个人的隐私，他们的个人数据在被允许访问的情况下会被披露。例如，一般公共利益的重要目标可包括保护国家安全和公共安全(例如关于潜在恐怖主义威胁或执法人员面临的严重风险的信息)；防止、侦查、调查或起诉刑事犯罪；并避免妨碍官方查询、调查和诉讼。与《公约》解释性报告第 146 段中对相称性的描述相似，在这方面，“相称性限制”预计将由各缔约国根据其国内法律框架的相关原则加以实施。对于《保护人权与基本自由公约》(《欧洲条约集》第 5 号)或修正《关于在个人数据自动处理方面保护个人的公约》的《欧洲委员会条约集》第 223 号议定书的缔约国，相称性应源自上述公约的要求。其他缔约国将适用其国内法律框架的相关原则，合理限制获得查阅的能力，以保护其他合法利益。如上所述，相称的限制必须保护他人的权利和自由，或保护一般公共利益的重要目标，并适当考虑到“有关个人的合法利益”。起草者认为“有关个人的合法利益”一语包括个人的权利和自由。在援引这些限制理由的情况下，鼓励被请求的官方机构为第 14 款的目的记录这一决定。缔约国还应考虑，如果任何限制的理由(例如，为保护机密或商业机密信息)仅适用于信息的某些部分，是否可以允许部分查阅。

273. 如果本条其他条款允许在第12款(a)项(1)目规定的条件下作出限制，“在裁决时”的意思，在第 7 款的情况下，指的是通知安全事件的时间点；在第 11 款(b)项的情况下，指的是提供个人通知的时间；在第 11 款(c)项的情况下，指的是缔约国要求保密的时间。

274. 根据第 12 款(a)项(1)目，每一缔约国应确保其数据已根据本议定书收到的任何个人，在其个人数据不准确或处理不当时，有权根据其国内法律框架中规定的程序，寻求并获得纠正，不得无故拖延。纠正应包括——在适当和合理的情况下，考虑纠正的理由和处理的特殊背景——纠正、补充(例如通过标记或通过提供额外或更正信息)、删除或匿名、限制处理或阻止。在这方面，起草者认为，如果数据的处理违反了第 5 款，删除或匿名属于适当合理的行动方案。在违反第2款的情况下，该缔约国也可限制处理；然而，这最终将取决于具体的背景(例如，需要为证据目的保留个人数据)。当数据匿名时，缔约国应考虑未经授权重新识别的风险，并采取适当措施，将该风险降至最低。鼓励各缔约国在可行的情况下，将所采取的任何纠正行动通知向其提供数据的缔约国和与之分享数据的其他实体。

275. 根据第12款(b)项，如果根据第12款(a)项拒绝或限制查阅或更正，缔约国应以书面形式(可以是电子形式)向有关个人提供答复，告知此人拒绝或限制的情况，不得无故拖延。虽然官方机构应提供拒绝或限制的理由，但必要时，为了不损害第 12 款(a)项(1)目所述的目标，通知可以是一般性的(即不确认或否认任何相关记录的存在)。但是，缔约国应确保通知包括关于现有补救方法的信息。

276. 当事人可以对获取信息收取费用(例如，收集和审查被要求获取的文件的行政费用)。然而，为了不劝阻或阻止使用，任何收费都应限于合理的范围，并且考虑到所涉及的资源，不得过高。为了方便行使第 12 款(a)项规定的权利，鼓励缔约国允许个人要求一名代表协助寻求和获得其中所述的措施，或代表本人提出请求和(或)投诉。在这种情况下，根据第 11 款(a)项发出的通知，以及根据第 12 款(a)项(1)目对查询请求作出的答复中获得的信息可提及这种可能性。然而，这种代表必须符合寻求采取此类措施或提出上述请求和(或)投诉的缔约国的国内适用法律要求，包括关于个人或实体代表他人合法利益的条件的规则(例如，在一些国内法律制度中，关于授权书的规则)。

第 13 款 司法和非司法补救措施

277. 第 13 款规定，“各缔约国均应制定有效的司法和非司法补救措施，为违反本条规定的行为提供补救”。对于违反本条规定的行为，应由各缔约国确定补救的类型，并不要求对每一违反本条的行为都提供一种类型的补救措施。所提供的补救措施必须有效处理违反本条的行为。

当事方可酌情将赔偿作为一种补救措施，以补偿索赔人已确定的侵权行为造成的人身或非人身损害。

第 14 款 监督

278. 第 14 款要求各缔约国“应设立一个或多个公共机构，对本条规定的措施单独或累积行使独立和有效的监督职能和权力”。该规定使缔约国在如何执行这一要求方面具有灵活性。一些缔约国可能设立专门的数据保护机构，而另一些缔约国可能选择通过一个以上的机构累积行使监督权，这些机构的职能可能重叠。这反映了各缔约国在宪法、组织和行政结构上的差异。在有些缔约国，这些监督机构可能设在其所监督活动的政府部门内，预算可能是该部门总预算的一部分。在这种情况下，这些机构应享有独立性，以便有效履行其监督职责。

279. 起草者认为，若干要素有助于独立和有效的监督职能和权力。主管部门应公正地执行任务和行使权力；它们应具备能力，不受可能干扰其独立行使权力和职能的外来影响；特别是在特定情况下，这些机构在行使调查权力和(或)采取纠正行动方面不应受到指示的制约；最后，这些机构必须具备履行职责所需的技能、知识和专长，并获得有效履行职责所需的适当财政、技术和人力资源。

280. 这些机构的职能和权力应“包括调查权、对投诉采取行动的权力以及采取纠正行动的能力”。起草者认为，调查权应包括获得履行任务所需信息的权力，包括在适当条件下查阅根据第 8 款保存的记录。纠正行动可包括对违规行为发出警告，或就如何使数据处理业务符合规定发出指示(例如要求实施额外的安全措施，以限制对数据的访问或纠正个人数据)、规定(暂时)中止某些处理操作或将该事项提交给其他权力机构(例如监察长、检察官、调查法官或立法机构)。此类纠正行动可由官方主动采取，或在个人就其个人数据的处理提出投诉时采取。

281. 鼓励缔约国促进各自监督机构之间的合作。缔约国各自主管机构在履行本条规定的监督职能时，可酌情进行协商。这可能包括交流信息和最佳做法。

第 15 款 协商和暂停

282. 第 15 款规定，根据第 14 条，当缔约国根据第 14 条第 1 款(a)项行事时，缔约国可暂停根据本议定书向另一缔约国转交个人数据。第 15 款明确指出，鉴于本议定书的重要执法目的，此种暂停只应在严格的条件下并按照其中所述的具体程序进行。本条的数据保护条款的目的是为保护个人数据提供适当的保障，包括在缔约国内部后续共享和后续转发的情况。起草者认为，该条的保障措施及其有效实施至关重要，因此认为，规定在某些情况下暂停个人数据的转交是重要的。因此，如果一方有大量证据表明存在系统性或实质性违反本条规定的行为，或即将发生实质性违反行为，则该方可暂停根据本议定书向另一方转交个人数据。虽然“确凿的证据”要求并不要求缔约国毫无疑问地证明存在系统性或实质性违约，但缔约国也不得仅凭怀疑或推测而暂停转交。相反，该方的决定必须有可信的事实证据的实质性支撑。“实质性违约”系指严重违反本条规定的重要义务。这可能包括缔约国未能在其国内法律框架中为本条规定所需的保障。起草者承认，也可以系统性违约为理由暂停，例如经常反复违反本条的保障措施。起草者进一步认识到，在没有重大违反行为的情况下，未能在在个别情况下适用与个人数据处理有关的某些保障措施，将不提供援引该条款的充分理由，因为有关个人应能够根据第 14 条第 13 款通过有效的司法和非司法补救措施来解决这类违反行为。

283. 第 15 款进一步规定，缔约国“在没有合理通知的情况下，不得暂停转交，在有关各方作出合理协商却未达成决议之前，不得暂停转交”。这一协商要求承认，只有在向另一方提供合理的机会，澄清情况或解决所表达的关切之后，才应暂停关键的执法转交。在协商开始时，援引第 15 款的一方可要求另一方提供有关信息。但是，如第 15 款所述，援引本款的一方必须事先掌握实质或系统性违约，或即将发生实质性违约的重要证据；因此，在怀疑有违规行

为时，不应利用协商机制来搜集进一步证据。只有经过合理通知和合理的协商期后未达成解决方案时，方可暂停转交依本议定书的数据。但是，如果发生系统性或实质性违约行为，对自然人的生命或安全构成重大和紧迫的风险，或对自然人的声誉或钱财造成重大和迫在眉睫的损害，缔约国可临时暂停转交。这包括对自然人的身体伤害或健康的重大和迫在眉睫的危险。在这种情况下，缔约国应在临时暂停转交后，立即通知另一方，并着手与之进行协商。起草者认为，临时暂停一般应限于与需要临时暂停的紧急情况直接相关的转交。

284. 如果暂停转交的一方满足第 15 款所列条件，可暂停转交，而另一方不得作出对等反应。但是，如果另一方有实质性证据证明，暂停方的暂停违反了第 15 款的规定，则可对等暂停向暂停方转交数据。在这种情况下，“确凿证据”一词的含义与暂停一方最初暂停时的含义相同。例如，如果暂停的一方并无“实质性证据”，违约行为既非“系统性的”，亦非“重大的”，或暂停履约的一方未能满足暂停的程序要求，特别是与协商有关的程序要求，那么暂停履约一方的暂停行为将违反第 15 款的规定。

285. 最后，第 15 款规定，“一旦证明暂停的违约行为得到纠正，暂停方应立即取消暂停”，并规定，“任何对等的暂停也应在此时取消”。适用于第 24 条第 4 款的一项类似规则，也适用于本款所述的暂停。换言之，第 15 款规定，“暂停前转交的任何个人数据应继续按照本议定书处理”。

286. 鼓励各缔约国就本款所述的任何暂停或临时暂停规定，向依据第二章第 2 节可向其发出请求或命令的服务供应商和实体作出公布或正式通知。这种通报对于有效暂停向严重或系统违反第 14 条的缔约国转交个人数据十分重要，而且对于确保服务供应商和实体不因误以为某一缔约国受这一暂停规定的约束而限制根据本议定书转交信息或证据也十分重要。

287. 虽然第 15 款规定了与以数据保护为由进行协商和暂停转交个人数据有关的具体程序，但第 15 款中的程序无意影响根据第 23 条第 1 款进行的协商，也无意影响根据国际法可能适用于本议定书其他条款的暂停权利。

第四章　最后条款

288. 本章所载条款大部分是根据 2017 年 7 月部长委员会第 1291 次部长代表会议通过的《欧洲委员会内部缔结的公约、附加议定书和修正议定书最后条款范本》和《公约》的最后条款制定的。由于本章下的一些条款使用了示范条款的标准用语，或者是以欧洲委员会长期的订约惯例为基础，因此不需要具体评论。但是，对标准示范条款的某些修改和对《公约》最后条款的某些偏离需要作出解释。

第 15 条　本议定书的效力

289. 第 15 条第 1 款(a)项纳入了《公约》第 39 条第 2 款。正如《公约》解释性报告第 312 段所承认的那样，该段指出，缔约国可自由适用已经存在的或将来可能生效的协议。本议定书与《公约》一样，一般规定了最低限度的义务；因此，该段承认，缔约国在就本议定书所涉事项建立关系时，除本议定书已规定的义务外，还可自由承担更具体的义务。但是，缔约国在这样做时必须尊重本议定书的目标和原则，因此不能接受有损于本议定书宗旨的义务。

290. 第 15 条第 1 款(b)项还承认，自 2001 年《公约》开放供签署以来，欧洲联盟(欧盟)的一体化程度有所提高，尤其是在刑事事项的执法和司法合作以及数据保护领域。因此，它允许欧盟成员国在彼此之间适用管辖本议定书所涉事项的欧盟法律。起草者希望欧盟法律包括欧盟法律秩序中规定的措施、原则和程序，特别是法律、条例或行政规定以及其他要求，包括法院

裁决。因此，第 1 款(b)项旨在涵盖欧盟成员国之间以及欧盟成员国与欧盟各机构、组织和机关之间的内部关系。如果没有与本议定书范围内的事项有关的欧盟法律，则本议定书将继续在属于欧盟成员国的缔约国之间管辖该事项。

291. 第 1 款(c)项明确指出，第 1 款(b)项并不影响本议定书在属于欧盟成员国的缔约国与其他缔约国之间的全面适用。因此，第 1 款(b)项无意在上文第 290 段所述的欧盟内部关系之外产生任何影响；本议定书在属于欧盟成员国的缔约国与其他缔约国之间完全适用。起草者认为，这一规定对于确保非欧盟成员国的缔约国在与欧盟成员国的缔约国的关系中获得本议定书的全部利益至关重要。例如，起草者讨论了从非欧盟缔约国收到信息或证据的欧盟成员国，在向另一个欧盟缔约国转交信息或证据之前，必须征得该非欧盟缔约国的同意，这与第 14 条第 10 款相一致。同样，本条第 1 款(a)项完全适用于属于欧盟成员国的缔约国和其他非欧盟成员国的缔约国。

292. 第 15 条第 1 款(a)项包含了《公约》第 39 条第 2 款。与《公约》类似，如《公约》解释性报告第 314 段所解释的那样，本议定书并不打算处理与缔约国之间或缔约国与私营实体之间在网路犯罪方面的合作形式，以及以电子形式收集刑事犯罪证据有关的所有未决问题。因此，在第 15 条第 2 款中纳入了明确的规定，即本议定书只影响其涉及的内容。不受影响的是可能存在但本议定书未涉及的其他权利、限制、义务和责任。

293. 第 15 条不包含类似于《公约》第 39 条第 1 款的规定。《公约》中的这一条款解释说，《公约》的目的是补充缔约国之间适用的双边条约或安排，包括某些引渡和互助条约。本议定书不包含任何引渡条款，其中有许多条款不是互助条款。正如第 5 条及其所附解释性报告中较详尽地解释的那样，第二章中合作措施的每一节都以不同的方式与互助条约相互作用。因此，起草人得出结论认为，他们无需列入类一项似于第 39 条第 1 款的规定。

第 16 条　签署和生效

294. 第 16 条允许《公约》所有缔约国签署并成为本议定书的缔约国。与《第一项议定书》(第 11 条)不同，本议定书没有规定加入本议定书的程序。希望签署并成为本议定书缔约国的国家必须首先成为《公约》的缔约国。

295. 第 3 款规定，本议定书应在《公约》五个缔约国表示同意接受本议定书约束三个月期满后的下个月的首生效。虽然《公约》第 36 条第 3 款规定，五个缔约国中至少有三个必须是欧洲委员会成员国《公约》才能生效，鉴于这是一项《公约》的附加议定书，所有缔约国都应享有同样的权利，只要至少有五个缔约国表示同意接受其约束，所有缔约国都应享有适用本议定书的同等权利，因而此处并没有列入这一要求。这遵循了《第一项议定书》第 10 条的做法。

296. 第 4 款说明了本议定书对其根据第 3 款生效后表示同意受其约束的《公约》缔约国生效的程序。这遵循了《公约》第 36 条第 4 款的做法。

第 17 条　联邦条款

297. 与《公约》第 41 条规定的联邦条款相类似，本议定书第 17 条载有一项联邦条款，允许属于联邦国家的缔约国“根据其中央政府与组成州或其他类似领土实体之间关系的基本原则”提出保留。第 17 条的目标与《公约》第 41 条的目标相同。也就是说，如《公约》解释性报告第 316 段所述，“照顾到联邦国家由于中央和地方当局之间权力分配的特点可能面临的困难”。

298. 允许联邦国家对《公约》第二章规定的义务(确立国内刑事犯罪和国内程序措施)提出保留，只要这些措施不属于联邦国家中央政府的管制权力范围。但是，联邦国家必须能够根据《公约》第三章向其他缔约国提供国际合作。

299. 虽然本议定书规定了国际合作而不是国内措施，但谈判者认识到，本议定书仍需要一项联邦条款。虽然《公约》没有为互助规定联邦制保留，但本议定书大部分措施的运作方式与传统的互助方式不同。本议定书提供了一些比传统互助更有效的合作措施，这些措施不一定需要中央政府参与。特别是，本议定书引入了两项措施，即第 6 条和第 7 条，它们规定一缔约国的主管机构可直接向另一缔约国的私营公司寻求合作。这些措施要求采取某些程序性步骤，而联邦国家可能难以要求其组成州或领土实体的主管机构遵守这些步骤。例如，第 7 条规定，一缔约国可通过通知秘书长，要求其他缔约国的官方在向寻求用户信息的服务供应商发送命令时，同时通知指定的政府主管部门。其他条款载有采取立法或其他措施的要求，而联邦国家可能无法要求其组成州或其他类似领土实体颁布这些措施。最后，本议定书载有详细的数据保护规定，而《公约》则没有。例如，在美国，根据其宪法和联邦制的基本原则，各组成州颁布各自的刑法和刑事诉讼法(独立于联邦法律)；设立各自的法院、检察官和警察；并调查和起诉本州的刑事犯罪。各州主管机构独立于联邦政府，不隶属于联邦政府。

300. 如果一联邦国家的组成州或类似领土实体的政府寻求本议定书规定的合作形式，则可能出现以下情况：(1)它们根据与中央政府不同的程序法和隐私权法运作；(2)它们在组织层次上不对中央政府负责；或(3)中央政府不具备法定权力指导它们的行动。在这种情况下，只有在下列情况下才能保证组成州或类似领土实体履行本议定书的要求——与寻求信息或证据有关的要求，以及与随后处理这些信息或证据有关的要求，倘若(1)其本身适用这些要求，或(2)如果其主管机构透过中央政府寻求合作，或在中央政府参与下确保这些要求得到履行(例如通过互助或全天候(24/7)联系点，或在中央政府参与联合调查组的情况下)。

301. 鉴于这些考虑，第 1 款为联邦国家缔约国提供了保留的可能性。此类缔约国，可以根据其关于中央政府与组成州或其他类似领土实体之间关系的基本原则，对承担本议定书规定的义务的权利作出保留，但须遵守限制这种保留范围的第 1 款(a)至 c 项。根据第 1 款(a)项，援引这项保留的联邦国家中央政府必须适用本议定书的所有条款(受现有保留和声明的限制)。关于本议定书规定的数据保护义务，对于根据第 14 条第 1 款(a)项行事的缔约国来说，这包括第 14 条第 9 款(b)项中关于后续与组成州或其他类似领土实体分享的义务(见解释性报告第 260 段)，在联邦政府根据本议定书要求提供信息的情况下，或者出于自身目的，或者代表联邦以下一级机构，并随后与联邦以下一级此类机构共享这一信息。此外，第1款(b)项规定，与《公约》第41条第1款类似，此种保留不应影响该联邦缔约国为其他缔约国根据第二章的规定所寻求的合作制订规定的义务。最后，根据第 1 款(c)项，尽管联邦国家提出保留，但本议定书第 13 条——根据《公约》第 15 条，该条要求根据国内法保护人权和自由——除适用于第 1 款(a)项所述的中央政府外，还适用于联邦国家的组成州或类似的领土实体。

302. 第 2 款规定，如果一联邦国家根据第 1 款作出保留，而该缔约国的组成州或类似领土实体的政府直接寻求另一缔约国的政府、供应商或实体的合作，则该另一缔约国“可阻止其领土上的主管机构、供应商或实体……予以合作”。另一方可决定以何种方式阻止其境内的主管机构或供应商或实体进行合作。另一方阻止合作的权力有两个例外。

303. 首先，第 2 款规定，如果由于组成州或其他类似领土实体履行了本议定书的义务，有关联邦缔约国已“通知欧洲委员会秘书长，其组成州或其他类似领土实体适用本议定书中适用于该联邦制国家的义务”，则该另一缔约国不得阻止合作。“本议定书中适用于该联邦制国家的义务”一语系指，组成州或类似领土实体的政府可以不受中央政府所不受的任何要求的约束，例如由于适用保留。如果联邦国家已就某一特定组成州向秘书长发出通知，则另一缔约国就须为执行来自该州的命令或请求作出规定，其程度与从中央政府收到的命令或请求相同。当然，第二章中各项合作措施所载的要求和程序仍然适用于这些组成州或类似领土实体提交的

请求或命令，而且必须遵守这些要求。本款要求欧洲委员会秘书长应设立并更新此类通知的登记册。鼓励缔约国向秘书长提供最新信息。

304. 其次，根据第 3 款，如果组成州或其他类似领土实体的请求或命令是通过中央政府提出的，或根据第 12 条在中央政府参与下达成的联合调查组协议提出的，另一缔约国不得以已作出第 1 款保留的联邦国家的组成州或类似领土实体正在寻求合作为由，阻止其领土上的主管机构、供应商或实体根据本议定书的规定转交信息或证据。这是因为，如果请求或命令是通过中央政府提交的，或者联合调查组协议是在中央政府的参与下签订的，那么就要求中央政府“应规定履行本议定书的适用义务”。由于中央政府正在提交请求或命令(或参与联合调查小组)，因此它有机会和义务核实本议定书关于这类措施的要求是否得到满足。例如，如果根据第 7 条第 5 款(a)项，必须通知另一缔约国转交寻求用户信息的命令，中央政府有义务提供这一通知。关于数据保护(对于根据第 14 条第 1 款(a)项行事的缔约国)，如果组成州或其他类似领土实体谋求通过中央政府进行合作，则中央政府向组成州或其他类似领土实体提供数据，且必须适用第 14 条第 9 款(b)项(在一缔约国内后续分享)中规定的要求。换言之，中央政府必须采取措施，以便接收部门通过提供与第 14 条所提供的保护水平相当的保护，继续有效地保护数据。以这种方式寻求和接收个人数据的组成州或类似领土实体的政府没有义务适用第 14 条。如果有关缔约国适用第 14 条第 1 款(b)项或(c)项所述的另一协议或安排，则应适用该协议或安排的适用条款。

305. 第 4 款与《公约》第 41 条第 3 款的条文和效力几乎相同。因此，关于《公约》的规定，其适用属于组成州或其他类似领土实体的管辖范围(除非已根据本条第 2 款向欧洲委员会秘书长发出通知)，联邦国家的中央政府必须：(1)将本议定书的规定告知这些州或其他类似领土实体的的主管机构；(2)提出其“赞成的意见，鼓励各州采取适当行动予以实施”，以鼓励各组成州或类似领土实体充分实施本议定书。就本议定书而言，这也是为了最终允许根据本条第 2 款通知这些组成州或其他类似领土实体。

第 18 条　适用领土

306. 《公约》第 38 条允许缔约国具体说明《公约》将适用的一个或多个领土。本议定书第 18 条自动适用于缔约国根据《公约》第 38 条第 1 款或第 2 款指定的领土，但以该声明未按照《公约》第 38 条第 3 款撤销为限。起草者认为，最好将《公约》和本议定书的相同领土范围作为默认规则适用。

307. 第 18 条第 2 款规定，“[一]缔约国在签署本议定书时，或交存批准书、接受书或核准书时，可说明本议定书不适用于该缔约国根据《公约》第 38 条第 1 款和第 2 款所作声明中指明的一个或多个领土”。根据第 3 款，缔约国可依照规定的程序撤销根据本条第 2 款作出的声明。撤销第 2 款中的声明，将产生对《公约》所涵盖但本议定书以前未适用的其他领土适用本议定书的效果。

308. 本条不允许将本议定书适用于《公约》未涵盖的领土。

第 19 条　保留和声明

309. 本条规定了某些保留的可能性。考虑到《公约》的全球影响力和本议定书实现成员数量相同的目标，这种保留使《公约》缔约国能够成为本议定书的缔约国，同时允许这些缔约国在适用的情况下保持符合其国内法、基本法律原则或政策考量的某些做法和概念。

310. 对保留的可能性加以限制，以确保缔约国尽最大可能统一适用本议定书。因此，除所列举的保留外，不得作出其他保留。此外，《公约》缔约国只能在签署本议定书或交存其批准书、接受书或核准书时提出保留。

311. 与《公约》一样，本议定书中的保留排除或修改了本议定书中规定的义务的法律效力(见《公约》解释性报告第315段)。在本议定书中，保留允许排除所有形式的合作。具体而言，第 7 条第 9 款(a)项允许一缔约国保留不完全适用第 7 条的权利。也允许保留排除为某些类型数据的整个条款的合作。具体而言，第 7 条第 9 款(b)项允许缔约国保留在披露某些类型的访问代码与其国内法律制度的基本原则相抵触的情况下，不对这些访问代码适用第 7 条的权利。同样，第 8 条第 13 款允许缔约国保留不对流量数据适用第 8 条的权利。

312. 第 19 条也提到声明。与《公约》类似，通过本议定书中的声明，允许缔约国纳入某些特定的附加程序，以修改条款的范围。这些附加程序的目的是适应某些概念、法律或实际差异，鉴于《公约》的全球影响力和本议定书企望的相同影响力，这些差异是合理的。列举的声明分为两大类。

313. 若干项声明允许缔约国宣布某些权力或措施必须由特定的主管机构执行，或通过特定的渠道传递合作。第 10 条第 9 款即属于这类情况(允许声明除向中央机关外，还可向其他机关提出请求)；第 12 条第 3 款(中央机关必须是联合调查组协议的签署方或以其他方式同意联合调查组协议)；第 8 条第 11 款(作出声明的缔约国可要求其他缔约国根据本条提出的请求，必须由其中央机关或由其他共同确定的机关转交)。

314. 第二类声明允许缔约国要求对某些合作措施采取单独或额外的程序步骤，以便遵守国内法，或避免给主管机构造成过重负担。例如，第 7 条第 8 款和第 9 条第 1 款(b)项允许一缔约国作出声明，要求其他缔约国就用户信息采取特定的程序步骤。第 7 条第 2 款(b)项和第 5 款(a)项、第 8 条第 4 款和第 9 条第 5 款允许采取额外的程序性步骤，以提供额外的保障或遵守国内法。声明的效果并不打算是对等的。例如，如果一缔约国根据第 10 条第 9 款作出声明——即根据本条提出的请求可送交除其中央机关以外的其他主管机构——其他缔约国可向作出声明的缔约国的其他主管机关提出请求，但作出声明的缔约国只能向其他缔约国的中央机关提出请求，除非这些中央机关也作出此种声明。

315. 本条第 2 款所列声明必须在缔约国签署或交存批准书、接受书或核准书时作出。相反，第 3 款所列声明可随时作出。

316. 第 3 款要求各缔约国按照本议定书第 7 条第 5 款(a)项和(e)项、第 8 条第 4 款和第 10 款(a)项和(b)项、第 14 条第 7 款(c)项和第 10 款(b)项以及第 17 条第 2 款规定的条件，将这些条款所述的任何声明、通知或函件通知欧洲委员会秘书长。例如，根据第 7 条第 5 款(e)项，“缔约国应在首次根据第 5 款(a)项通知欧洲委员会秘书长时，向秘书长通报该机构的联系方式”。

缔约国还应将第 8 条第 10 款(a)项和(b)项所指的“机构”通知欧洲委员会秘书长。已指示秘书长建立并不断更新缔约国指定的这些机构的名册，并指示缔约国确保为该名册提供的详细内容一向准确无误(见第 7 条第 5 款(f)项和第 8 条第 12 款)。

第 20 条　保留的地位和撤回

317. 与《公约》第 43 条一样，该条没有规定具体的时限，要求缔约国在情况允许时尽快撤回保留。为了对缔约国保持一定的压力，使它们至少考虑撤回保留，第 2 款授权欧洲委员会秘书长定期询问撤回保留的前景。这种询问的可能性是欧洲委员会若干文书的现行做法，并反映在《公约》第 43 条第 3 款和《第一项议定书》第 13 条第 2 款中。因此，缔约国有机会表明它们是否仍需维持对某些条款的保留，并随后撤回那些不再需要的保留。希望随着时间的推移，各缔约国将能够尽可能多地撤销保留，以促进本议定书的统一执行。

第 21 条　修正

318. 第 21 条采用的程序与《公约》第 44 条规定的修正程序相同。这一简化程序允许在必要时进行修正，而无需就修正议定书进行谈判。不言而喻，根据本条第 3 款与《公约》缔约国进行协商的结果对本议定书缔约国不具有约束力。如《公约》解释性报告第 323 段所述，“修正程序大多被认为是针对程序性和技术性相对较小的修改”。

第 22 条　争端的解决

319. 第 22 条规定，《公约》第 45 条规定的争端解决机制也适用于本议定书(见《公约》解释性报告第 326 段)。

第 23 条　缔约国协商和执行情况评估

320. 第 23 条第 1 款规定，《公约》第 46 条(缔约国协商)适用于本议定书。根据《公约》解释性报告第 327 段，第 46 条为缔约国提供了一个框架，以便就本公约的执行情况、与计算机或计算机相关犯罪主题有关的重大法律、政策或技术发展的影响、以电子形式收集证据以及补充或修正本公约的可能性进行协商。将该程序设计为灵活的，由缔约国决定如何以及何时举行会议。2004 年《公约》生效后，各缔约国开始定期召开《网络犯罪公约》委员会(《公约》委员会)会议。随着时间的推移，根据第 46 条和《公约》缔约国通过的《议事规则》设立的《公约》委员会，对缔约国执行《公约》的情况进行了评估，通过了指导性说明，以促进缔约国就《公约》的施用达成共识，并编写了本议定书草案。缔约国的协商程序保持了灵活性，因此本议定书缔约国可酌情作出调整，以考虑到执行本议定书可能产生的需要。

321. 与《公约》类似(见解释性报告第 327 段)，根据第 23 条进行的协商应“审查在使用和执行《公约》过程中出现的问题，包括……作出的声明和保留的影响”。这可包括根据第 17 条第 2 款通知欧洲委员会秘书长的联邦国家组成州或类似领土实体对本议定书执行情况的协商和评估，而作为欧盟成员的缔约国应就其根据第 15 条第 1 款(b)项使用和执行本议定书的情况,向本议定书其他缔约国通报适用的欧盟法律并与之协商。除下一款所述的通过本条所述的这些程序可进行协商外，缔约国还可在双边基础上进行协商。对于联邦国家，这些协商和评估将通过其中央政府进行。

322. 第 23 条第 2 款规定了在第 46 条和上文讨论的《公约》委员会规定的更大框架内，审查本议定书使用和执行情况的具体程序。第 2 款规定，“缔约国应定期评估本议定书各项规定的有效适用和执行情况”，并指出，2020 年 10 月 16 日修订的《网络犯罪公约委员会议事规则》第 2 条将指导这些评估。关于这些程序，可查阅《公约》委员会网站。由于《公约》委员会审查了《公约》的若干条款，并根据这些程序发布了报告，起草者认为，这些既定程序应比照适用于对本议定书条款的评估。鉴于本议定书缔约国承担的额外义务及其规定的独特合作措施，起草者决定，只有本议定书缔约国才能进行这些评估。鉴于评估本议定书某些条款的使用和执行情况所需的相关专业知识，包括关于数据保护的第 14 条，缔约国可考虑让其相关专题专家参与评估。

323. 一方面，此类评估的规则需要是可预测的，但实际经验可能会导致需要调整这些程序，而无需根据第 21 条对本议定书进行正式修正。因此，第 2 款规定，对这些程序的初次审评应在本议定书生效五年后进行，届时缔约国可协商一致修改这些程序。缔约国在初步审查之后的任何时候，可以协商一致方式修改这些程序。

324. 鉴于第 14 条所载的数据保护保障措施的相关性，起草者认为，一旦在本议定书下有了充分的合作记录，就应尽快对第 14 条进行评估，以有效审查缔约国对这一条款的使用和执行情况。因此，第 3 款规定，一旦有十个《公约》缔约国表示同意接受本议定书的约束，即应着手对第 14 条进行评估。

第 24 条　退约

325. 第 24 条第 1 款和第 2 款与《公约》第 47 条相似，无需进一步解释。第 3 款规定，“本议定书缔约国退出《公约》即构成对本议定书的退约”。鉴于本议定书强调分享信息或证据，其中可能包括个人数据，起草者认为，谨慎的做法是增加第 4 款，以澄清“在退约生效日期之前转交的信息或证据应继续按照本议定书的规定处理”。