联合国 A/77/196

大 会

Distr.: General
20 July 2022
Chinese
Original: Spanish

第七十七届会议

议程项目 69 (b)

促进和保护人权：人权问题，包括增进人权和基本自由切实享受的各种途径

隐私权

秘书长的说明

秘书长谨向大会转递隐私权特别报告员安娜·布里安·努格蕾蕾斯根据人权理事会第 28/16 号决议编写并提交的报告。

22-11362 (C) 140822 190822

摘要

隐私和保护个人数据的基本原则是与这些问题有关的法律制度的结构性组成部分，因为它们的双重职能是解释和整合监管框架。这些原则是使数据控制方和处理方能够适当处理个人信息的最重要和最有用的手段，特别是在面临滥用信息和通信技术的风险情况下。

本报告分析了合法性和正当性、同意、透明度、目的、公正性、相称性、最小化、优质、责任和安全性等原则，因为这些原则是与隐私和保护个人数据有关的整个法律制度的基石。本报告对 7 份国际规范性文件中的这些原则的系统阐述进行了以下比较研究。它还强调了这些原则的共同方面，以着力于在全球一级实现统一，并应对将保护隐私和个人数据作为一项基本人权的艰巨难题，这一基本人权由于具有跨领域性质，因此能够保护其他基本人权，如数字时代的自由、平等、荣誉和尊严等权利。

隐私和保护个人数据的基本原则

一. 导言

1. 与隐私和数据保护有关的指导原则构成了解释准则，有助于填补法律空白，对于确定如何解决使用信息和通信技术处理个人数据时出现的问题至关重要。

2. 这一领域的国家和国际法规具有普遍性。因此，在无论是国家或国际一级的公共或私营部门以及无论使用何种技术的控制方和处理方的各种个人数据处理活动中，都必须使这些法规具有具体的形式。[1] 一个关键目标是有效执行有关法规，因为在民主政府制度中，仅仅承认和制定有关基本权利的法律是不够的。这些神圣的权利必须伴随着有效的保护保障，而不论其背景如何。

3. 因此，本报告将分析的指导原则是确保适当处理个人信息的最重要和最有用的手段。

4. 隐私和保护个人数据的基本原则不应被视为仅仅是建议，因为它们的地位高于建议。由于这一地位，它们是涉及这些问题的法律制度的结构性组成部分。这些原则要求控制方和处理方在处理个人数据时采取适当行动，并应对滥用信息和通信技术、人工智能和其他技术发展的风险，从而使数据主体能够保持对其个人信息的控制。

5. 这些原则是密切相关的。因此，不仅必须对它们进行单独审查，而且必须将其作为其所属一套原则的一部分进行审查，以确保对个人信息的适当管理，同时维护相关权利和基本自由。

6. 应当考虑到特殊类别的个人数据，尤其是敏感数据。目前的共识是，应对这类数据实行处理方面的限制，因为它们涉及个人生活中最隐私的领域，需要更大的保护。因此，其处理过程可能对权利和基本自由构成更大的风险。

7. 根据国际规范性文件，在大多数国家，一般情况下不应处理敏感数据，除非法律特别允许。这一规则的存在是为了消除差别对待数据主体的风险。

8. 法律最好说明敏感个人数据的类别，并确定其保护范围和例外情况。各国在确定哪些数据属于这些类别时，也理应考虑到文化、社会和政治背景以及当地现实情况。

9. 当敏感的个人数据得到法律的适当保护时，应允许处理这些数据。此类保证必须特别包括需要坚持与隐私和数据保护有关的指导原则。

[1] “鉴于科技创新的速度，技术中立性尤其重要并有助于确保立法仍然能够配合未来的发展，而不会过快地过时。”联合国国际贸易法委员会，*Building confidence in electronic commerce: legal issues in the international use of electronic authentication and signature methods* (维也纳，2009 年)。

10. 为了开始在全球一级制定隐私和保护个人数据的原则，本报告分析了 7 个相关国际规范性文件中规定的指导原则。

11. 本报告强调了这些文件的基本共同点以及一些具体特点，目的是寻求共识，以便能够协调妥善处理个人数据的努力，同时在数字时代维护保护此类数据、隐私和尊严的权利。

二. 监管分析

12. 以下各节分析了合法性、依法性和正当性、同意、透明性、目的、公正性、相称性、最小化、质量、责任和安全性等原则。这一分析基于以下文件：

- 《欧洲联盟数据保护总条例》(总条例)[2]
- 《欧洲委员会关于在处理个人数据方面保护个人的现代公约》(现代《第 108 号公约》)[3]
- 大会题为“电脑个人数据档案的管理准则”(联合国准则)的第 45/95 号决议
- 伊比利亚美洲数据保护网采用的《伊比利亚美洲国家个人数据保护标准》[4] (《伊比利亚美洲标准》)
- 欧洲委员会关于经济合作与发展组织《保护隐私和个人数据跨界流动准则》(《经合组织准则》)的建议[5]
- 亚洲太平洋经济合作组织隐私框架(亚太经合组织隐私框架)[6]
- 美洲国家组织(美洲组织)大会通过的附带注解说明的《美洲法律委员会隐私和个人数据保护最新原则》(《美洲组织原则》)[7]

[2] 2016 年 4 月 27 日欧洲议会和欧洲委员会 2016/679 号条例(欧盟)。

[3] 可查阅 http://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1。

[4] 伊比利亚美洲数据保护网，“Standards for Personal Data Protection for Ibero-American States”。可查阅 http://https://www.argentina.gob.ar/sites/default/files/estandares_eng.pdf。

[5] 可查阅 http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation。

[6] 可查阅 http://www.apec.org/publications/2017/08/apec-privacy-framework-(2015)。

[7] 美洲法律委员会的报告，“Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with annotations”，2021 年 4 月 9 日。

合法性、依法性和正当性原则

13. 根据这一原则，个人数据在其整个有效周期内的处理必须由责任方根据相关法律在尊重国际公认的人权的情况下进行。这意味着，通过对个人数据的适当、从而合法的处理，将确保尊重隐私和其他权利以及数据主体的尊严。

14. 个人数据受保护权被认为是一项能够保护其他权利的权利，[8] 维护这一权利将确保适当处理有关个人意愿的数据，从而保障尊重他或她的其他基本权利。

15. 虽然合法性必须是个人数据整个有效周期中从收集到删除的所有处理活动的基础，但重点通常置于第一次处理活动即数据收集，因为如果这一活动是非法进行的，它将影响由此产生的其他处理活动的合法性。[9]

16. 现代《第 108 号公约》规定，数据处理在所有阶段都必须秉持合法的目的，并且必须依法进行(第五.1 条)。

17. 根据《联合国准则》，按照合法、公平的原则，个人信息的收集和处理必须合法、公正。

18. 各种国际规范性文件一直在扩展和吸纳与合法性原则相关并对该原则进行补充的其他数据保护原则。

19. 在这方面，《总条例》第 6 条和叙文第 39 和 40 条规定，数据处理在根据法律确立的法律依据进行时是合法的。

20. 《伊比利亚美洲标准》规定，根据正当性原则，个人数据只能在法律规定的条件下处理(第 11 条)。

21. 根据《经合组织准则》，必须以合法和公正的手段并在数据主体知情或同意的情况下收集数据(第 7 条)。

22. 处理个人数据的合法性取决于是否存在适用法规中规定的合法理由。表 1 列出了国际公认的合法理由，是根据对相关国际规范性文件的分析编制的。

[8] 现代《第 108 号公约》第一条。

[9] 《经合组织准则》第 7 段；《美洲国家组织原则》第一原则；《准则》第 1 条。

表 1
数据处理的合法理由

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲组织附带注解说明的《隐私和个人数据保护最新原则》
	条	条	条	条	段	原则	原则
数据主体的同意	五.2		11.1 (a)	6.1 (a)	10 (a)	三.24	一
数据主体同意用于与收集数据的目的不相符的目的		3 (b)					一
法律	五.3		14.1		10 (b)	四.25 (c)	一
控制方的法律义务			11.1 (f)	6.1 (c)			一
履行合同或合同前步骤			11.1 (e)	6.1 (b)		四.25 (b)	一
公共利益			11.1 (h)	6.1 (e)			一
控制方的正当利益			11.1 (i)	6.1 (f)			一
数据主体或第三方的重大利益			11.1 (g)	6.1 (d)			一
在公共当局面前确认或维护数据主体的权利			11.1 (d)				一
法院命令、裁决或公共当局的授权			11.1 (b)				一

23. 下文按照所分析的国际规范性文件中提及的允许处理个人数据的理由的频率，列出了此类理由。

24. 有 6 份文件将数据主体的同意作为处理个人数据的正当理由之一，使其成为所分析的法规中最常提及的理由。

25. 根据《联合国准则》，同意并未确定为一个通常允许的理由，而是作为收集数据目的以外的目的进行处理活动的理由。考虑到这一点和《联合国准则》第 1 条(其中涉及所审议的原则)，必须按照《联合国宪章》的宗旨以公正和合法的方式处理个人数据。这包括确保进行一定程度的宣传，并告知数据主体。

26. 数据主体同意之后是法律或每个成员国国内法的授权，即 5 份文件中提到的理由。

27. 有 4 份文件将履行合同或合同前步骤列为合法理由。在数字时代的经济背景下，确认这些与社会和商务关系以及电子商务有关的理由特别重要。

28. 有 3 份文件确认控制方的法律义务、公共利益、控制方的正当利益以及数据主体或第三方的重大利益为合法理由，两份文件将在公共当局面前承认或维护数据主体的权利以及法院命令、裁决或公共当局的授权作为合法理由。

29. 为了维护保护个人数据、隐私和尊严的权利，无论监管背景如何，数据控制方和处理方(如适用)必须满足相关的允许理由之一，才能管理个人数据。

同意原则

30. 同意是一种明示或默示的意愿表示，同意方受其法律约束。当数据主体给予同意时，其作为这些数据的主体对其个人数据的控制权力就直接显现出来。

31. 同意原则与合法性原则密切相关，因为它是国际公认的处理个人数据的最常见的允许理由。

32. 根据同意原则，数据主体必须表明他们接受其个人数据可以被收集、记录、处理、交流或传输，而且一般来说，这些数据可用于包括删除在内的任何处理活动，从而授予控制方决定数据整个有效周期的权力。[10]

33. 在所分析的规范性文件中，同意是处理个人数据的最重要正当理由之一，因为在这些文件中有 6 份文件具体确定了这一点，并具有各种特点。[11]

34. 下文所述的内容是一种界定可以给予同意的参照系的方法，以便尽可能忠实地反映数据主体的意愿。

35. 下表 2 比较了 7 个相关国际规范性文件中提到的特点。

表 2

同意的特点

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
	条	条	条	条	段	原则	原则
自由的	五.2			4.11			二
具体的	五.2		12	4.11			二
知情的	五.2			7.3 和 4.11	备忘录第 52 点		二
明确的	五.2		12	4.11			二
可撤回的			12.2	7.3			二

36. 如上标所示，在正在审议的文本中，现代《第 108 号公约》、《总条例》[12]和《美洲国家组织原则》赋予保护个人数据所需的同意类型最多的特点，以确保数据主体的意愿得到忠实反映。

37. 根据对文本中所提到的特点的分析，这种同意必须是自由的、具体的、知情的、明确的和可撤回的。虽然现代《第 108 号公约》和《联合国准则》(第 4 条)、《经合组织准则》及《亚太经合组织隐私框架》(第 21 至 23 条和第 26 条)似乎都

[10] 《总条例》叙文 32。

[11] 如关于合法性、依法性和正当性原则的前一节所述，《联合国准则》仅将同意确立为为收集数据目的以外目的进行处理活动的正当理由。

[12] 第 4.11 条；6.3(a)和(b)条；6.1(a)、(b)、(c)、(d)和(e)条；7 和 8 条。

没有可撤回性，但可在这些文本中与数据主体权利有关的章节中找到。[13] 在这些文本中，可撤回性被视为同意权力的一种关联因素，具有与给予同意相反的效果，而且发生在给予同意之后。

38. 就《经合组织准则》而言，知情同意的概念原则上不是产生于条款的措辞，其中规定在适用情况下，必须在数据主体知情或同意的情况下收集数据。然而，《经合组织准则解释性备忘录》指出，虽然可能需要或不需要主体的同意，但知情是最低要求。[14] 因此，当收集个人数据需要征得同意时则必须告知，因为数据主体的知情是必须满足的最低要求。

39. 在关于同意原则的条款中，并不总是出现授权处理数据的意愿表达的特点。然而，在某些文件中，如《总条例》(第 4 条)，在定义和叙文中列出了某些此类特点。

40. 《联合国准则》和《亚太经合组织隐私框架》没有确定同意的特点。

41. 作为允许处理个人数据的理由，必须在开始所允许的处理活动之前获得同意。

42. 同意原则与透明性原则直接相关，因为数据主体的有效同意意味着他或她已被适当告知其个人信息将受哪些条件制约。

43. 必须要提到文件中反映同意处理未成年人个人数据的方式。就个人数据的保护而言，儿童和青少年被认为是一个脆弱群体，特别容易受到处理与其有关的信息的后果的影响。因此，必须确保他们得到全面保护和福祉。

44. 《伊比利亚美洲标准》(第 13 条)、《总条例》(第 8 条)和《美洲国家组织原则》(第二原则)指出，未成年人的同意须经亲权持有人或其法律代表的授权，因为这些人对处理的后果负责。这些文件还规定，每个国家的国内法可规定未成年人在适当保障下可直接表示同意的最低年龄。

透明性原则

45. 与处理个人数据相关的原则之一是，控制方必须透明地处理数据主体的相关数据。根据这一原则，控制方必须从收集时起就告知主体其个人信息将面对的处理条件，以便主体能够对数据行使应有的控制。

46. 下表 3 显示了控制方必须向数据主体提供如所分析的国际规范文件中所示的信息。

[13] 现代的《第 108 号公约》第九条；《联合国准则》第 4 条。

[14] 《解释性备忘录》(第 52 点)，第 19 页。

表 3

必须向数据主体提供的信息

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《数据保护总条例》		《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
				当数据获取自主体时	当数据不是获取自主体时			
	条	条	条	条		段	原则	原则
控制方和/或代表的身份和地址	八.1 (a)		16.2 (a)	13.1 (a)	14.1 (a)	12	21 (d)	二
数据处理有无特点和/或主要特点			16.1			12	21 (a)	
法律基础或依据	八.1 (b)			13.1 (c)	14.1(c)和 14.2(b)			二
处理的目标或目的	八.1 (b)		16.2 (b)	13.1 (c)	14.1 (c)	12	21 (b)	二
所处理数据的类别	八.1 (c)				14.1 (d)			
当数据不是获取自主体时的数据来源			16.2 (e)		14.2 (f)			
接收方或接收方类别	八.1 (d)		16.2 (c)	13.1 (e)	14.1 (e)		21 (c)	二
关于权利和行使权利的方式的信息	八.1 (e)		16.2 (d)	13.2 (b)和(c)	14.2 (c)和(d)		21 (e)	二
向监管当局提出申诉的权利				13.2 (d)	14.2 (e)			
数据传播是否是法定要求或合同要求，或者是否是签订合同所必需的，主体是否需要提供其个人数据以及不提供的后果				13.2 (e)				
是否存在自动化决策，包括概况分析、有关所涉逻辑的实质信息以及这种处理的重要性和预期后果				13.2 (f)	14.2 (g)			
当计划为收集数据目的以外的目的进行进一步处理时，关于目的的信息				13.3	14.4			
数据保护干事的联系方式				13.1 (b)	14.1 (b)			
储存期限或用于确定该期限的标准				13.2 (a)	14.2 (a)			
是否计划进行传播或传输，以及授权此类传播或传输的条例				13.1 (f)	14.1 (f)			
待传输的信息								
传输的目的			16.2 (c)					

47. 如上所示，在所分析的 7 份国际规范性文件中，《联合国准则》没有提到透明性原则。因此，下文的分析侧重于在其余 6 份文件中反复提及的信息，这些信息被确定为必须提供给数据主体的，以维护透明性原则。

48. 所有 6 份文件中都指出必须披露控制方或其代表的身份和地址以及数据处理的目标或目的。这些数据是透明性的根本基础。

49. 在 5 份文件中规定，必须披露数据主体的权利和可能行使这些权利的方式，以及接收方或接收方类别。关于主体需要了解其这种权利的问题，文件中提到主体必须能够适当对与其有关的个人信息实行控制。

50. 在 3 份文件中规定，必须披露处理的法律基础或依据，以及处理是否存在特点和/或主要特点。

51. 无论数据处理的法律依据如何，都必须遵守透明性原则。在向数据主体提供信息的及时性方面，[15] 或当数据主体不是所收集的个人信息的来源时，[16] 可能会出现例外情况，但必须以确保尽可能大的透明性和公平性为目的而作出此类例外。

52. 两份文件中规定，必须披露所处理数据的类别以及并非直接从数据主体获得的数据的来源。

53. 本分析还包括仅在一份国际规范性文件中确定需要告知数据主体的信息，以便为该主体提供行使其控制权的更好条件。

54. 《伊比利亚美洲标准》在传输目的方面和《总条例》在下列信息方面的情况即如此：数据保护干事的联系方式；储存期限或用于确定该期限的标准；是否计划进行传播或传输以及授权此类传播或传输的条例；向监管当局提出申诉的权利；数据传播是否是法定要求或合同要求，或者是否是签订合同所必需的，主体是否需要提供其个人数据以及不提供的后果；是否存在自动化决策，包括概况分析、有关所涉逻辑的实质信息以及这种处理的重要性和预期后果；当计划为收集数据目的以外的目的进行进一步处理时，有关该目的的信息。

55. 在仅包含在《总条例》中的信息类型中，有一类特别值得注意，即旨在确保数据主体了解处理与其相关的信息的方式(例如是否涉及人工智能)、并向其提供“关于所涉逻辑的实质信息”和“重要意义和预期后果”的信息。[17]

[15] 《亚太经合组织隐私框架》第 22 条。

[16] 现代的《第 108 号公约》第八.3 条。

[17] 西班牙数据保护局。*Alignment of processing operations involving artificial intelligence with the General Data Protection Regulation: an introduction*。2020 年 2 月，第 24 页。可查阅 https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf。

56. 数据主体按照透明性原则必须知晓的信息，必须以简单、清晰、易懂、易于获取和可理解的语言提供；[18]在这方面必须特别注意儿童和青少年的情况。[19]

57. 控制方在管理个人信息时的正确行为也特别重要，因为他们必须制定透明的个人数据处理政策。[20]

目的原则

58. 目的原则指导并界定了从收集到删除的所有个人数据处理活动。一般来说，目的将由数据控制方定义。但如果控制方没有正当的理由处理数据，则不会被视为控制方。

59. 从收集阶段开始，其目的必须符合所分析的国际规范性文件中规定的某些特点。目的必须明确、具体、正当和相关。一旦符合法规中为定义目的而确立的特点，这些特点就可以作为个人数据将面临的处理活动的定义符。

60. 根据目的原则，所收集的数据只能在其收集目的范围内使用。该原则用于限制从收集到存储、修改、传播、传输和任何其他处理活动直至数据的删除等各种处理活动。

61. 因此，正如各种规范性文件所指出的，[21] 任何处理活动都不得超出最初界定的目的所允许的范围，除非根据适用的条例和必要的保障措施得到明确授权。《亚太经合组织隐私框架》[22] 就是一个例子，其中提到数据可能被用于与最初确定的目的相一致的其他目的。

62. 在所分析的所有文本中，[23] 都确立了目的原则，并阐述了其特点和实际应用的后果。该原则与合法性或依法性原则密切相关，因为它将正当性确定为目的的一个基本特点。

63. 国际规范性文件指出，为了允许数据处理，目的必须满足哪些特点。如下表所示，目的必须是明确、具体、正当和相关的。

[18] 《伊比利亚美洲标准》第 16.3 条；《总条例》第 12.1 条；《亚太经合组织隐私框架》第 21 条。

[19] 《伊比利亚美洲标准》第 16.3 条；《总条例》第 12.1 条；

[20] 《伊比利亚美洲标准》第 16.4 条；《经合组织准则》第 12 条；《亚太经合组织隐框架》第 21 条。

[21] 现代《第 108 号公约》第五.4 (b) 条；《联合国准则》第 3 条；《伊比利亚美洲标准》第 17 条；《总条例》第 5.1(b)条；《经合组织准则》第 9 段；《亚太经合组织私隐架构》第 24 和 25 条；《美洲国家组织原则》第一原则。

[22] 《亚太经合组织隐私框架》第四部分第 25 条。

[23] 现代《第 108 号公约》第五十四(b) 条；《联合国准则》第 3 条；《伊比利亚美洲标准》第 17 条；《总条例》第 5.1(b)条；《经合组织准则》第 9 条；《亚太经合组织私隐架构》第 24 和 25 条；《美洲国家组织原则》第一原则。

表 4
目的的特点

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
	条	条	条	条	段	原则	原则
明确的	五.4 (b)	3	17	5.1 (b)	9	24 和 25	一
具体的	五.4 (b)	3	17	5.1 (b)	9	24 和 25	
正当的	五.4 (b)	3	17	5.1 (b)		24 和 25	一
相关的	五.4 (b)	3	17	5.1 (b)	9	24 和 25	

64. 在上述规定中，只有《经合组织准则》第 9 段没有将正当性列为数据处理目的的一个特点。这可能是简单的起草问题造成的，也可能是遗漏了根据对整个规范性文件的分析似乎是隐含的内容。

65. 关于《美洲国家组织原则》，虽然第一原则的文本中没有明确规定所有目的的特点，但从该原则的注释中可以清楚地看出，这些特点都包括在该原则之下。

66. 关于与目的有关的数据处理的特殊性，应当指出，《总条例》(第 5.1 条)、《伊比利亚美洲标准》(第 17.3 条)、现代《第 108 号公约》(第五.4(b)条)和《美洲国家组织原则》(第四原则)规定可能会将数据用于收集数据目的以外的目的，但这些目的以统计、历史或科学为目的。

67. 如上所述，为数据处理提供理由的正当目的界定了控制方和处理方的行动(如需行动的话)。因此，一旦目的已经用尽或实现，继续处理数据就不再正当，除非适用法规中明确规定了此类处理，在这种情况下，此类规定将成为新的允许理由。

公正原则

68. 这一原则涉及到必须忠实地按照为收集个人信息提供理由的所有条款和条件处理这种信息并使用有助于实现这一目标的处理方法。

69. 以下是对规定这一原则的国际规范性文件的分析。

70. 《联合国准则》第 1 条规定了合法性和公正性的原则。其目的是确保数据不以非法或不公正的方式处理以及不将其用于违背《联合国宪章》原则的目的。一般而言，这意味着不应任意歧视数据主体；数据处理应按照国家和国际原则和规则进行；个人的权利应得到切实尊重。

71. 在《伊比利亚美洲标准》中，这就是“忠诚原则”(第 15 条)。根据该条，控制方有义务给予主体利益受保护的权利，并避免通过欺骗或欺诈手段处理数据。处理个人数据导致对主体的不公平或任意歧视被视为不公正。

72. 同样，《总条例》第 5.1(a)条规定，在处理个人数据时必须遵循公正原则，以及与数据主体有关的合法性和透明性原则。

73. 《经合组织准则》在数据收集限制原则下提到了公正性(第 7 段)。该条涉及两个问题：(a) 数据收集的限制；(b) 与数据收集方法有关的规定，并就该规定指明数据须以合法及公正的方法获取。

74. 《亚太经合组织隐私框架》第 24 条间接提到了公正原则，该条规定收集手段应当合法和公正。

75. 同样，虽然现代《第 108 号公约》没有明确提到这一原则，但可以通过第五.4(a)条的规定推断出这一原则的确立，该条规定在处理数据时，应公正地使用数据。此一条件不仅适用于第一个处理活动(收集)，而且适用于涉及数据处理的任何活动。

76. 最后，在《美洲国家组织原则》中，这项原则被确立为第一原则“合法目的和忠诚”的一部分，根据这项原则，“个人数据的收集只应用于合法目的，并以忠诚与合法的手段进行”。在这种情况下，在收集个人数据所用手段的问题上明确规定了公正性。

77. 《美洲国家组织原则》指出，“忠诚是有背景的，取决于具体情况”，即必须为个人提供关于如何及何时提供个人数据的适当选择，且不得通过欺诈、欺骗或以虚假借口获取数据。

78. 所有个人数据处理活动都必须做到公正。以收集为重点的国际规范性文件中强调，不正确或非法的初始行动会标明和界定后续处理活动的特点。

79. 毫无疑问，控制方和处理方的行动必须以在个人数据的整个有效周期内公正处理为特点，而无论背景或使用的技术为何。公正行事涉及责任、道德和遵守根据这些原则时所适用的规则。

相称性原则

80. 相称性原则对个人数据的处理实施了限制。根据这一原则，个人数据以及此类数据所面对的处理活动必须仅用于实现数据收集的目的。[24]

81. 必须铭记，从早在决定是否进行处理之时起的数据处理所有阶段都必须遵守这一原则，以从收集阶段一开始就确保这一过程是适当合法的。

82. 与这一原则密切相关的是目的原则和最小化原则，前者规定数据的处理应符合收集数据的目的，后者规定数据应保持在实现既定目的所需的最低限度。

[24] 现代《第 108 号公约》第五.1 条和五.4 (c)条；《伊比利亚美洲标准》第 18.1 条；《亚太经合组织隐私框架》第 24 条；《总条例》第 5.1 (c)条；《联合国准则》第 3 (a)条；《经合组织准则》第 9 段；《美洲国家组织原则》第三和第四原则。

83. 相称性原则的一项要求是，控制方必须进行评价以便从可用于实现授权目的的各种处理操作中选择对隐私的侵犯最少的操作。当涉及到使用某些可能对基本权利构成风险的信息和通信技术时，这种评价就变得特别必要。

84. 这一原则在所分析的所有国际规范性文件中都有规定，如《伊比利亚美洲标准》第 18 条的具体规定，或在其他原则之下的规定。以下文书中的原则之下涵盖了这一原则：《联合国准则》中明确目的的原则(第 3(a)条)；现代《第 108 号公约》中数据处理的正当性和数据质量的原则(第五.1 和五.4(c)条)；《总条例》中最小化原则的一部分(第 5.1(c)条)；《亚太经合组织隐私框架》中的收集限制原则(第 24 条)；《经合组织准则》中的目的说明原则(第 9 段)；《美洲国家组织原则》中的相关性和必要性原则(第三原则)和有限处理和保留原则(第四原则)。

85. 从表 5 可以看出，在《伊比利亚美洲标准》、《总条例》、《联合国准则》和《美洲国家组织原则》中，都提到了数据与目的的相关性。此外，现代《第 108 号公约》、《伊比利亚美洲标准》、《总条例》和《美洲国家组织原则》中规定，数据必须适合于目的。

86. 在所分析的所有国际规范性文件中，除《联合国准则》外，都以这样或那样的方式规定，数据应受到限制，而且就收集数据的目的而言，数据不应过量。《伊比利亚美洲标准》、《总条例》、《亚太经合组织隐私框架》和《美洲国家组织原则》中规定，数据应限于目的所需的数量。

87. 现代《第 108 号公约》中规定，数据不得超出处理这些数据的目的范围。它还规定，数据必须与目的相关，数据处理必须与所追求的正当目的相称。《经合组织准则》规定，数据的使用应限于实现数据收集时所说明的目的或与这些目的不相符的其他目的。

表 5

构成相称性原则的限制

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
	条	条	条	条	段	原则	原则
适用于目的	五.4 (c)		18.1	5.1 (c)			三
与目的相关	五.4 (c)	3(a)	18.1	5.1 (c)			三
有限且不超出目的	五.4 (c)		18.1	5.1 (c)	9	24	三

88. 在如《伊比利亚美洲标准》、《亚太经合组织隐私权框架》、《总条例》和《联合国准则》等一些国际规范性文件中，在这一原则的范畴内明确提到了“个人数据”。在如《经合组织准则》等其他文件中，提到了对这类数据的“处理”，而还有一些文件如现代《第 108 号公约》和《美洲国家组织原则》，既提到个人数据本身，也提到将对这些数据进行的处理。

89. 尽管有上述提及并考虑到国际规范性文件的完整文本，必须结合所收集的个人数据和将对这些数据进行的处理活动审查相称性原则。数据及其处理都必须是适当、相关的，并限于收集数据的正当目的。

最小化原则

90. 最小化原则是指在任何时候都必须将数据限制在实现既定目的所需的范围内。

91. 在这方面，该原则与目的原则密切相关，这是限制待处理数据量的一个参照。

92. 《总条例》是唯一明确规定最小化原则的文书。其第五.1(c)条规定，个人数据应是充分、相关的并仅限于处理这些数据的目的所必需的。在所分析的其他文件中，[25] 该原则的内容被列为相称性原则或一些其他原则的一部分。

93. 最小化原则还与《总法规》为控制方和处理方规定的某些义务有关，如设计和默认的隐私。最小化作为一种预防措施，有助于降低安全漏洞的风险及其对数据库的影响。

94. 如《总条例》第 25.2 条所述，“控制方应采取适当的技术和组织措施，确保在默认情况下仅处理每一具体处理目的所需的个人数据。这项义务适用于所收集的个人数据的数量、处理的范围、储存的期限和可读取性。”

95. 鉴于越来越频繁地使用信息和通信技术来处理个人数据，必须更加积极地遵守最小化原则。

质量原则

96. 质量原则要求数据必须准确、精确、完整和最新，这意味着数据控制方必须采取措施确保数据准确、精确、完整和最新。这一原则在一些国际规范性文件中被称为准确性[26] 或完整性原则。[27]

97. 如下表 6 所示，在整个处理过程中，个人数据必须准确、完整和精确，必须在必要时更新，无论是由控制方或处理方主动更新，还是应数据主体的要求更新。

[25] 《伊比利亚美洲标准》第 18 条；《联合国准则》第 3 条；现代《第 108 号公约》第五.1 和五.4(c)条；《亚太经合组织隐私框架》第 24 条；《经合组织准则》第 9 段；《美洲国家组织原则》第三和第四原则。

[26] 《联合国准则》第 2 条和《美洲国家组织原则》第七原则。

[27] 《亚太经合组织隐私框架》第 27 条。

表 6
数据质量的特点

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
	条	条	条	条	段	原则	原则
准确/精确	五.4 (d)	2	19.1	5.1 (d)	8	27	七
最新	五.4 (d)	2	19.1	5.1 (d)	8	27	七
完整		2	19.1		8	27	七

98. 现代《第 108 号公约》第五.4(d)条规定，数据必须准确且并不断更新。《联合国准则》第 2 条提到核查数据的准确性和相关性的义务；确保其继续尽可能完整，以避免遗漏错误；并确保予以定期更新。

99. 如下所示，在 5 个国际规范性文件中，质量原则明显与目的原则挂钩。

100. 《伊比利亚美洲标准》第 19 条规定，控制方有义务采取“必要措施保持个人数据……准确、完整和最新，从而其真实性不被改变，以按要求符合处理数据的目的。”

101. 《总条例》规定，个人数据应准确，必要时应及时更新，并规定必须采取一切合理措施，确保删除或纠正与处理这些数据的目的有关的不准确的个人数据(第 5.1(d)条)。

102. 《经合组织准则》(第 8 段)和《亚太经合组织隐私框架》(第 27 条)均提到数据应准确、完整和保持最新。《美洲国家组织原则》在数据准确性原则方面规定，“数据应保持准确、完整和最新，以满足数据处理的目的，从而不影响其真实性”(第七原则)。

103. 所处理的个人信息的质量对于恰当地实现为收集该信息以及随后处理该信息提供依据的目的至关重要。确保数据质量是实现授权目的的责任标志。

104. 为了充分遵守质量原则，数据控制方和处理方必须在其组织内采取措施确保其收集和管理的个人数据准确、精确、完整或充分并保持最新，以便在充分尊重个人数据主体的权利的同时实现授权目的；这将对他们自己有利。无论数据主体为了确保他人正在处理的其信息的质量而决定采取什么行动，都要做到这一点。

责任原则

105. 责任原则可以从两个角度加以分析：第一，控制方和处理方必须建立遵守隐私和数据保护原则的机制，保护和保障数据主体的权利和自由；第二，控制方和处理方必须能够保证并证明遵守了这些原则。

106. 就所分析的国际规范性文件而言，《伊比利亚美洲标准》确立了责任原则(第 20 条)；该条规定，控制方必须建立所有必要的机制，以遵守这些标准中规定的原则和义务，并就个人数据的处理向数据主体和监管当局负责。为此，控制方可

利用标准、国家或国际最佳做法、自我管制或认证制度或其认为适当的任何其他机制。上述手段也适用于处理方的数据处理期间和数据传输期间。

107. 《伊比利亚美洲标准》第 20.3 条列举了控制方为遵守责任原则可采用的机制的例子。控制方应不断审查和评价这类机制，以评估其在确保遵守适用的国家法律方面的效力。

108. 这一原则是在《总条例》的“问责制”一词下确立的(第 5.2 条)。它可以被定义为控制方有必要或有义务实施适当的技术和组织措施，以确保和证明个人数据的处理是根据《条例》进行的(第 24 条)，特别是合法、公正和透明的原则；目的限制；数据最少化；准确性；储存限制；完整性及保密性。为此，控制方应制定程序以确保规则的适用，并能够向第三方证明《条例》得到有效适用和遵守(第 5.2 条)。

109. 《总条例》规定了确保遵守该原则的若干措施，包括通过设计和默认实施数据保护(第 25 条)；保存处理活动的记录(第 30 条)；实施安全措施(第 32 条)；将安全漏洞通知监管当局和数据主体(第 33 和 34 条)；进行数据保护影响评估(第 35 条)；指定一名数据保护干事(第 37 条)。

110. 在上述措施中，当处理对数据主体的权利和自由构成高度风险时，需要按照《总条例》的规定进行数据保护影响评估(第 35 条第 1、3 和 4 段)。[28] 在使用新技术处理自然人的数据时，这一点尤其重要。

111. 控制方必须在处理个人数据之前进行评估，以帮助做出相关决策并符合数据保护的设计和默认要求。[29]

112. 问责制原则要求各组织分析其处理的数据类型、处理目的和所进行的处理操作的类型。根据这些信息，他们必须明确确定如何实施《总条例》所要求的措施，确保这些措施和程序足以履行数据保护要求，以及如何向数据主体和监管当局证明其遵守情况。这一原则要求各组织对其实施的所有个人数据处理操作采取负责任、尽职和积极主动的态度。[30]

113. 同样，《美洲国家组织原则》强调需要通过、实施和展示安全措施，重点是个人数据和国际数据传播和传输安全的问责制，控制方负责确保持续的保护水平符合这些《原则》(第十原则)。

---

[28] 《总条例》第 35.3 条：“在下列情况下，尤其需要进行第 1 款所述的数据保护影响评估：(a) 对自然人的个人方面进行的系统和广泛的评价，这种评价基于包括特征分析的自动化处理，并以此为基础作出对该自然人产生法律效力或同样对该自然人产生重大影响的决定；(b) 大规模处理第 9 (1)条所述特殊类别的数据，或处理与第 10 条所述刑事定罪和犯罪有关的个人数据；(c) 对公众可访问的领域进行大规模的系统监测。”

[29] 关于涉及 2016/679 号条例(欧盟)，WP.248 的目的的数据保护影响评估以及如何确定数据处理是否“可能导致高风险”的准则。2017 年 4 月。第 16 页。

[30] 西班牙数据保护局，“What is the principle of proactive responsibility?”, www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva。

114. 《经合组织准则》规定，控制方有责任遵守隐私保护规则和决定，必须遵守《准则》确立的各项原则(第 14 条)。

115. 《亚太经合组织隐私框架》也涉及这一原则，主要侧重于数据传输(第 32 条)。当个人信息被传输给无论是国内还是国际上的另一个人或组织时，控制方都应获得数据主体的同意，或在未获得同意的情况下应确保接收方将始终如一地保护信息，并应根据各项原则采取合理步骤确保信息在传输后得到保护。

116. 现代《第 108 号公约》规定，控制方和处理方必须采取技术和组织措施，在处理的所有阶段考虑到保护个人数据权的影响(第十.1 和十.3 条)。《公约》的解释性报告列出了控制方和处理方可能必须采取的措施，包括培训雇员；确立适当的通知程序；说明何时必须删除数据；为实施《公约》而订立委托处理的具体合同条款；建立内部程序以便能够核查和证明遵守情况。[31]

117. 除《联合国准则》外，所分析的所有国际规范性文件都具体提及这一原则。只有《伊比利亚美洲标准》和《总条例》确立了为确保遵守这一原则而需要采取的机制或措施，如下表 7 所示。

表 7
责任原则和确保遵守的机制

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
	条	条	条	条	段	原则	原则
具体提及责任原则	十.1		20	5.2	14	32	十
确定为确保遵守原则而需要采取的机制或措施			20.3	5.1、24、25、30、32、33、34、35 和 37			

118. 从本质上讲，责任原则倾向于加强对数据保护和隐私原则和条例的遵守，控制方和处理方必须在所开展的所有处理活动中遵守这些原则和条例，并确保客观要素在信任和尊重所涉基本权利的氛围中成为支持真正的遵守和实现正当目的的支柱。

安全性原则

119. 安全是数据保护的根本；没有安全就没有数据保护。

120. 为了确保遵守这一原则，必须识别、评价和记录个人数据有效周期中可能出现的风险，以便实施必要的安全措施，并能够保证个人数据的机密性、完整性和可用性，避免任何风险。

[31] 对《公约》的解释性报告，第 10 条，第 85 段。可查阅 http://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a。

121. 所分析的所有国际规范性文件都或多或少地提及了这一原则，并指出需要制定适当、充分、及时、合理或充足的安全措施，以防止各种类型的风险，如对个人数据未经授权的读取以及这类数据的丢失、更改、销毁或披露。[32]

122. 表 8 列出了每项国际规范性文件中提到的安全措施和风险的类型。该表还说明了哪些文件载有确定应采取措施的准则，哪些文件规定了报告违反安全行为的义务。

表 8
安全性原则

	《关于在处理个人数据方面保护个人的现代公约》	《联合国电脑个人数据档案的管理准则》	《伊比利亚美洲数据保护网个人数据保护标准》	《欧洲联盟数据保护总条例》	《经合组织保护隐私和个人数据跨界流动准则》	亚太经合组织隐私框架	美洲国家组织附带注释的《隐私和个人数据保护原则》
安全措施类型	适当的安全措施(第七.1 条)	适当措施(第 7 条)	充分的行政、实物和技术措施(第 21.1 条)	适当的技术或组织措施(第 5.1(f)条)	合理的安全保障(第 11 段)	适当的保障措施(第 28 段)	合理和适当的技术、行政或组织安全保障措施(第六原则)
风险类型	意外或未经授权地读取、销毁、丢失、使用、更改或传播个人数据(第七.1 条)	意外损失或破坏等自然危险，以及未经授权的读取、欺诈性滥用数据或计算机病毒污染等人为危险(第 7 条)	个人数据的损坏、丢失、更改、销毁、读取以及一般的任何非法或未经授权的使用(第 22.1 条)	未经授权或非法处理以及意外丢失、销毁或损坏(第 5.1(f)条)	数据的丢失或未经授权的读取、销毁、使用、修改或披露(第 11 段)	丢失或未经授权的读取，或未经授权的销毁、使用、修改或披露或其他滥用(第 28 条)	未经授权或非法的处理，包括读取、丢失、销毁、损坏或披露，即使是意外发生(第六原则)
确定采取何种措施的准则			第 21.2 条	第 32 条		第 28 条	
向监管当局通报违反安全行为	第七.2 条		第 22 条	第 33 条	第 15(c)段	第 54 条	
向数据主体通报安全违规行为			第 22 条	第 34 条	第 15(c)段	第 54 条	

[32] 表 8 列示了这一信息，其中列出了文件中所引用的条款中提到的安全措施和风险的类型(现代《第 108 号公约》第七.1 条；《联合国准则》第 7 条；《伊比利亚美洲标准》第 21.1 条；《总条例》第 5.1(f)条；《经合组织准则》第 11 段；《亚太经合组织隐私框架》第 28 条；《美洲国家组织原则》第六原则。

123. 安全措施必须与风险的大小相称；应得到定期审查和更新，也可予以审计，以改进和防止过时。[33]

124. 《美洲国家组织原则》规定，安全措施应受到长期审查和更新(第六原则)，而《伊比利亚美洲标准》规定，控制方应采取行动保证定期监测、修订、维持和不断改进适用于个人数据处理的安全措施(第 21.3 条)。《亚太经合组织隐私框架》规定，应定期审查和重新评估安全措施(第 28 条)。

125. 各种国际规范性文件都规定了向监管当局通报安全违规行为的义务，包括现代《第 108 号公约》(第七.2 条)、《伊比利亚美洲标准》(第 22 条)、《总条例》(第 33 条)、《经合组织准则》(第 15(c)段)和《亚太经合组织隐私框架》(第 54 条)。除现代《第 108 号公约》外，这些文件还规定了向有关数据主体通报安全违规行为的义务。

126. 必须强调通报监管当局以及在适当情况下通报数据主体的重要性。这使监管当局能够确保在发生安全违规行为的情况时采取适当措施，并确保尽快遏制违规行为；还确保受安全违规行为影响的数据主体知悉有关的违规行为及可能由此造成的损害。

127. 西班牙数据保护局指出，根据《总条例》中的安全性原则，要求数据处理方进行风险分析，以确定需要实施的技术和组织措施，从而保证其处理的个人数据的完整性、可用性和保密性。[34]

128. 《伊比利亚美洲标准》(第 21.2 条)、《总条例》(第 32 条)和《亚太经合组织隐私框架》(第 28 条)规定了如下所述的确定应执行的安全措施的准则或因素，但都没有规定应采取的具体措施，因为这样做不可能避免不过时。

129. 《总条例》中规定，控制方和处理方在确定确保与风险相称的安全水平的适当措施时，应考虑以下因素：“最新技术水平、实施费用和数据处理的性质、范围、背景和目的，以及自然人的权利和自由受到不同可能性和严重性损害的风险”(第 32 条)。

130. 《伊比利亚美洲标准》也提到这些因素，并增加了以下内容：已进行或将进行的个人数据的国际传输；数据主体的数目；数据泄露对数据主体可能造成的后果；以前的泄露事件(第 21.2 条)。

131. 《亚太经合组织隐私框架》规定，安全措施应与恐将造成的损害的可能性和严重性、信息的敏感性和持有信息的背景相称(第 28 条)。《隐私框架》与其他国际规范性文件不同，规定只有控制方负责基于上述因素实施和维护安全措施，而没有提及处理方。

[33] 《美洲国家组织原则》第六原则。

[34] 西班牙数据保护局，《原则》，2021 年 11 月 25 日，www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios。

132. 《美洲国家组织原则》中没有以上述方式阐述安全性原则。然而，这些原则规定，“为保护个人数据而采取的措施的选择应考虑到如下因素：㈠ 这些措施对数据主体权利可能产生的影响，特别是未经授权的第三方可能从这些数据中发现的潜在价值；㈡ 与实施措施有关的费用；㈢ 数据处理的目的；㈣ 正在处理的个人数据、特别是敏感数据的性质”(第六原则，注解)。

133. 在所分析的国际规范性文件中，只有《总条例》提供了确保与风险相称的安全水平的技术和组织措施的例子，即：“(a) 个人数据的假名化和加密；(b) 确保处理系统和服务的持续保密性、完整性、可用性和复原力；(c) 在发生物理或技术事故时，及时恢复个人数据的可用性和读取的能力；(d) 定期测试、评估和评价确保处理安全的技术和组织措施的有效性的流程”(第 32.1 条)。

134. 《总条例》第 32.3 条规定，遵守行为守则或建立认证机制可用于证明对这些要求的遵守情况。

135. 所有控制方和处理方必须采取措施确保个人数据的安全性，并保护个人数据免遭未经授权的读取、丢失、更改、破坏、披露或损坏等风险。如果不采取安全措施，个人信息容易受到这些风险的侵害，可能会对数据主体的权利造成严重损害。因此，所分析的所有国际规范性文件都提到需要针对可能出现的风险制定各种措施；在某些情况下，它们甚至提供了确定应采取的适当安全措施的准则，但没有具体说明确切的措施，因为不可能更新各项文件以跟上技术进步和可能发生的违规行为。

136. 为了以负责任和合乎道德的方式评价风险和数据控制方在其正当授权范围内以及无疑需要对其负责处理的个人数据适当保密的情况下应采取的适当安全措施，必须考虑到各种技术的多样性及其动态变化，以提高其收集和处理数据的能力。

137. 为了避免严重侵犯数据主体的权利的行为，必须确保个人数据的完整性、可用性和保密性，这是数据控制方和处理方的责任。如果发生违规行为，应尽可能减少对数据主体权利的影响；当发生违规行为时则须依循各项准则，例如告知监管当局及相关数据主体的规定。

三. 结论

138. 作为隐私和个人数据保护基础的指导原则是与这些问题有关的法律制度的构成部分。这些原则作为解释的准则，有助于填补法律空白并要求控制方和处理方在处理个人数据时采取适当的行动。

139. 合法性必须是个人数据整个有效周期中所有处理活动的基础，并基于适用法规中确立的正当理由。

140. 同意原则与合法性原则密切相关，因为这是国际公认的处理个人数据的最常见的许可理由。

141. 无论数据处理的法律基础如何，都必须遵守透明性原则。

142. 在所分析的所有规范性文件中都确立了目的原则。目的必须明确、具体、正当和相关。它的职能是将对个人数据进行的处理活动的定界符。

143. 公正原则要求在处理个人信息时忠实遵守为收集个人信息提供依据的所有条款和条件，并使用有助于实现这一目标的处理方法。

144. 根据相称性原则，个人数据的使用以及对此类数据进行的处理活动必须完全是为了实现为之收集数据的正当目的。

145. 正在处理的个人信息的质量对于正确实现该信息的收集及其后续处理的目的至关重要。

146. 责任原则倾向于加强对原则和法规的遵守，并确保客观要素在信任和尊重所涉基本权利的氛围中成为真正的遵守和实现合法目的的基础。

147. 没有安全，就没有数据保护，也没有对隐私的尊重。确保个人数据的完整性、可用性和保密性是一项重要任务和主要责任。必须考虑到技术的多样性及其动态变化，从而以负责任和合乎道德的方式评价风险和适当的安全措施。

148. 国际规范性文件在涉及隐私和个人数据保护原则方面有许多共性。

149. 所确定的共同要素可作为达成全球共识的基础，从而有可能以协调和适当的方式应对个人数据处理过程中出现的各种挑战，如国际数据传输、信息和通信技术的使用以及人工智能；人权应该在虚拟和面对面的环境中得到同等尊重。

150. 在当前的全球化和数字化时代，有必要继续在处理个人数据所涉及的不同利益之间找到平衡方面取得进展，以寻求监管合作和协调。