2021/0106（COD）

关于欧洲议会和欧盟理事会制定有关人工智能的统一规则（《人工智能法》）以及修订若干联盟立法的建议

朱悦（译）
同济大学法学院 上海市人工智能社会治理协同创新中心

2024年1月19日，欧盟委员会、欧洲议会和欧盟理事会共同完成了《人工智能法》的定稿。对全球范围内人工智能乃至整个数字经济的发展来说，这一立法具有非同寻常的重要性。故第一时间译出，以供初步的参考。之后也将随时根据反馈修订译本，并将很快推出结合整个立法过程的逐条研究。值得补充的是，尽管实质内容已经定稿，由于细节还在完善之中，若干标点和文字还有遗漏讹误，少许编号存在从-1而非1开始、字母和数字混合编号、重复不连续等问题。这些讹漏不影响内容，将在后续版本通过融贯性检查逐步修正。

有关后续的内容，《人工智能法》距离正式生效理论上还有五道步骤。一是通过欧洲议会相关委员会和全体会议表决，预计在4月10号完成。二是通过欧盟理事会相关委员会和全体会议表决，预计在3月或之前完成。三是由欧洲议会主席和欧盟理事会主席分别签署。四是刊宪。三和四取决于行政的安排，通常需要几个月的时间，五是自刊宪后二十日起生效。目前来看，除了有关公共场合（实时）人脸识别和通用目的人工智能的部分条款仍有很小的“再起波澜”的可能性，这些流程再对《人工智能法》内容产生实质影响的概率微乎其微。

欧洲议会和欧盟理事会，
考虑到《欧洲联盟运作条约》，特别是其中的第16条和第114条，
考虑到欧盟委员会的建议，
向国家议会递交法律草案后，
考虑到欧洲经济和社会委员会的意见，[1]
考虑到欧洲中央银行的意见，[2]
考虑到欧洲数据保护委员会和欧洲数据保护监督员的联合意见，
考虑到地区委员会的意见，[3]
按照普通立法程序行事，
鉴于：

(1) 本条例的目的是改善内部市场的运作，特别是为联盟内符合联盟价值观的人工智能系统的开发、投放市场、投入使用和使用制定统一的法律框架，促进以人为本和值得信赖的人工智能的应用，同时确保对健康、安全和《欧盟基本权利宪章》（《宪章》）所规定的基本权利的高度保护，包括民主和法治以及环境的保护，防止人工智能系统在联盟内产生有害的影响，并且支持创新。本

[1] 官方公报[……]，[……]，第[……]页。
[2] 参考欧洲中央银行的意见。
[3] 官方公报[……]，[……]，第[…….]页。

条例确保基于人工智能的商品和服务的跨境自由流动，从而防止成员国对人工智能系统的开发、营销和使用施加限制，除非本条例明确加以授权。
(1a) 本条例的适用应符合《宪章》所载的欧盟价值观，促进对个人、公司、民主和法治以及环境的保护，同时促进创新和就业，并且使得欧盟成为采用可信人工智能的领导者。
(2) 人工智能系统可以很容易地部署在经济和社会的众多部门，包括以跨国界的方式部署，并在整个联盟内流转。一些成员国已在探索通过国家规则的方式，以确保人工智能的可信度和安全性，并确保其开发和使用符合基本权利的义务。不同的国家规则可能会导致内部市场支离破碎，降低开发、进口或使用人工智能系统的运营商的法律确定性。因此，为了实现可信赖的人工智能，应确保在整个欧盟范围内提供一致和高水平的保护，同时应根据《欧洲联盟运作条约》第114条，规定经营者的统一义务，保证在整个内部市场统一保护压倒一切的公共利益和个人权利，从而防止出现阻碍人工智能系统及相关产品和服务在内部市场自由流通、创新、部署和使用的分歧。如果本条例包含关于在处理个人数据方面保护个人的具体规则，涉及限制为执法目的使用人工智能系统进行远程生物特征识别、为执法目的使用人工智能系统对自然人进行风险评估以及为执法目的使用人工智能系统进行生物特征分类，则就这些具体规则而言，本条例宜以《欧洲联盟运作条约》第16条为依据。有关这些具体规则和对《欧盟运作条约》第16条的援引，应咨询欧洲数据保护委员会。
(3) 人工智能是一个快速发展的技术族，能够为各行各业和社会活动带来广泛的经济、环境和社会效益。通过改进预测、优化运营和资源配置，以及为个人和组织提供个性化的数字解决方案，人工智能的使用可以为公司提供关键的竞争优势，并支持有益于社会和环境的成果，例如在医疗保健、农业、食品安全、教育和培训、媒体、体育、文化、基础设施管理、能源、运输和物流、公共服务、安全、司法、资源和能源效率、环境监测、生物多样性和生态系统的保护和恢复，以及减缓和适应气候变化等领域支持响应成果。
(4) 同时，根据其具体应用、使用情况和技术发展水平，人工智能可能会产生风险，并对受欧盟法律保护的公共利益和基本权利造成损害。这种损害可能是物质性的，也可能是非物质性的损害，包括身体、心理、社会或经济损害。
(4a) 鉴于人工智能可能对社会产生的重大影响以及建立信任的必要性，人工智能及其监管框架的发展必须符合《欧洲联盟条约》第2条所载的欧盟价值观、各项条约和《宪章》所载的基本权利和自由。作为前提条件，人工智能应是以人为本的技术。人工智能应作为人类的工具，最终目的是提高人类福祉。
(4aa) 为了确保在健康、安全和基本权利方面对公众利益提供一致和高水平的保护，应为所有高风险人工智能系统制定统一规则。这些规则应与《宪章》保持一致，并应是非歧视性的，且符合欧盟的国际贸易承诺。这些规则还应考虑到《欧洲数字权利宣言》和《数字十年原则》（2023/C 23/01）以及人工智能高级别专家组的《值得信赖的人工智能的伦理准则》。
(5) 因此，需要制定一个联盟层面的法律框架，规定关于人工智能的统一规则，以促进内部市场开发、使用和吸收人工智能，同时满足对公共利益的高度保护，如健康和安全以及对基本权利的保护，包括联盟法律承认和保护的民主、法治和环境保护。为实现这一目标，应制定规范某些人工智能系统的市场投放、投入使用和使用的规则，从而确保内部市场的顺利运作，并使这些系统能够受益于商品和服务自由流动的原则。这些规则应明确而有力地保护基本权

利，支持新的创新解决方案，使欧洲的公共和私人行为者能够创建符合欧盟价值观的人工智能系统生态系统，并释放欧盟所有地区数字化转型的潜力。本条例规定了这些规则以及支持创新的措施，尤其关注包括初创企业在内的小微型企业，从而支持欧盟理事会[4]提出的目标，即促进欧洲以人为本的人工智能方法，并在安全、可信和合乎道德的人工智能发展方面成为全球领导者，同时确保按照欧洲议会[5]的具体要求保护道德原则。

(5a) 本条例中规定的关于人工智能系统的市场投放、投入使用和使用的统一规则应适用于各个部门，并且，根据其采取的新立法框架的方法，不应影响现有的联盟法律，特别是关于数据保护、消费者保护、基本权利、就业和工人保护以及产品安全的法律，本条例是对这些法律的补充。因此，这些欧盟法律规定的消费者和其他可能受到人工智能系统负面影响的人的所有权利和救济措施，包括根据1985年7月25日关于有关缺陷产品责任的法律、法规和行政规定的相近的理事会85/374/EEC号指令对可能的损害进行赔偿的权利和救济措施，不受影响且完全适用。此外，在就业和工人保护方面，本条例不应影响欧盟有关社会政策的法律以及与欧盟法律不一致的国家劳动法，这些法律涉及就业和工作条件，包括工作场所的健康和安全以及雇主和工人之间的关系。本条例也不应影响行使成员国和联盟承认的基本权利，包括罢工或采取成员国特定劳资关系制度所涵盖的其他行动的权利或自由，以及根据国家法律进行谈判、缔结和执行集体协议或采取集体行动的权利。本条例不应影响[COD 2021/414/EC]指令中旨在改善平台工作条件的规定。此外，本条例旨在通过制定具体的要求和义务，包括人工智能系统的透明度、技术文件和记录保存方面的要求和义务，加强现有权利和救济措施的有效性。此外，本条例对参与人工智能价值链的各经营者所规定的义务，应在不影响国家法律的情况下适用，这些国家法律符合欧盟法律，具有限制使用特定的人工智能系统的效力，但这些法律不属于本条例的范围，或追求的是本条例所追求的目标之外的其他的合法公共利益目标。例如，考虑到联合国关于儿童权利的第25号一般性意见只要国家劳动法和未成年人（例如未满18岁的个人）保护法并非专门针对人工智能系统并追求其他合法的公共利益目标，就不应受到本条例的影响。

(5aa) 保护个人数据的基本权利尤其受到2016/679号条例和2018/1725号条例以及2016/680号指令的保障。2002/58/EC号指令还为保护私人生活和通信保密性，包括为终端设备中存储和访问的任何个人和非个人数据设定了条件。这些欧盟法案为可持续和负责任的数据处理提供了基础，包括数据集中包含个人数据和非个人数据的情况。本条例无意影响有关个人数据处理的现行欧盟法律的适用，包括有权监督这些文件的遵从状况的独立监督机构的任务和权力。只要人工智能系统的设计、开发或使用涉及个人数据的处理，本条例也不影响人工智能系统的提供者和部署者作为数据控制者或处理者所承担的义务，这些义务源自国家或欧盟关于保护个人数据的法律。此外，还需说明的是，数据主体继续享有此类联盟法律赋予他们的所有权利和保障，包括与完全自动化的个人决策相关的权利，其中也包括画像相关的权利。根据本条例制定的关于人工智能系统投放市场、投入使用和使用的统一规则，应有助于有效实施并使数据

[4] 欧盟理事会，欧盟理事会特别会议（2020年10月1日和2日）结论，EUCO 13/20，2020年，第6页。

[5] 欧洲议会2020年10月20日决议，其中向委员会提出了关于人工智能、机器人和相关技术伦理问题的框架建议，2020/2012(INL)。

主体的权利和其他救济措施得以行使，这些权利和救济措施受关于保护个人数据和其他基本权利的欧盟法律的保障。
(5ab) 本条例不应影响欧洲议会和理事会2000/31/EC号指令[经《数字服务法》修订]中有关中介服务提供者责任的规定。
(6) 本条例中的人工智能系统概念应明确界定，并与从事人工智能工作的国际组织的工作密切配合，以确保法律的确定性，促进国际趋同和广泛接受，同时提供灵活性，以适应该领域的快速技术发展。此外，这一概念应基于人工智能系统的关键特征，这些特征使其有别于较简单的传统软件系统或编程方法，不应涵盖仅基于自然人所定义的规则自动执行操作的系统。人工智能系统的一个主要特点是具有推理能力。这种推理指的是获得输出的过程，如预测、内容、建议或决策，也指人工智能系统从输入/数据中推导出模型和/或算法的能力，人工智能系统还可以影响物理环境和虚拟环境。在构建人工智能系统时，能够进行推理的技术包括：从数据中学习如何实现特定目标的机器学习方法；从待解决任务的编码知识或符号表示中进行推理的基于逻辑和知识的方法。人工智能系统的推理能力不仅限于基本的数据处理、学习、推理或建模。
“基于机器”一词指的是人工智能系统在机器上运行这一事实。明确或隐含目标的提法强调，人工智能系统可以根据明确界定的目标或隐含目标运行。人工智能系统的目标可能不同于人工智能系统在特定环境中的预期目的。就本条例而言，环境应被理解为人工智能系统运行的背景，而人工智能系统产生的输出则反映了人工智能系统执行的不同功能，包括预测、内容、建议或决定。
人工智能系统在设计上具有不同程度的自主性，这意味着它们的行动在一定程度上独立于人类的参与，并具有在没有人类干预的情况下运行的能力。人工智能系统在部署后可能表现出的适应性是指自主学习能力，允许系统在使用过程中发生变化。人工智能系统可以独立使用，也可以作为产品的一个组成部分，无论该系统是实际集成到产品中（嵌入式），还是为产品的功能服务而不集成到产品中（非嵌入式）。
(6a) 本条例中提到的“部署者”概念应解释为在授权下使用人工智能系统的任何自然人或法人，包括公共机关、机构或其他团体，但在个人非职业活动中使用人工智能系统的情况除外。根据人工智能系统的类型，该系统的使用可能会影响到部署者以外的人。
(7) 本条例中使用的生物识别数据的概念应根据欧洲议会和理事会2016/679 号条例第4条第14项[6]、欧洲议会和理事会2018/1725号条例第3条第18项[7]、欧洲议会和理事会2016/680号指令第3条第13项[8]而定义。生物识别数据可用于自然人的认证、识别或分类，以及自然人情感的识别。
(7a) 本条例中使用的生物识别的概念应界定为自动识别人的身体、生理和行为特征，如面部、眼球运动、体形、声音、韵律、步态、姿态、心率、血压、气

[6] 欧洲议会和欧盟理事会 2018 年 10 月 23 日 2018/1725 号条例，关于在欧盟机构、团体、办公室和机关处理个人数据时保护自然人，以及关于此类数据的自由流动，并废除 45/2001 号条例和 1247/2002/EC 号的决定（官方公报，295，2018 年 11 月 21 日，第 39 页）
[7] 欧洲议会和欧盟理事会 2016 年 4 月 27 日关于在主管机关为预防、调查、侦查或起诉刑事 犯罪或执行刑事处罚而处理个人数据时保护自然人以及关于此类数据自由流动的 2016/680 号指令，并废除理事会 2008/977/JHA 号框架的决定（《执法指令》）（官方公报，119，2016 年 5 月 4 日，第 89 页）。
[8] 欧洲议会和欧盟理事会2016年4月27日关于在个人数据处理方面保护自然人以及关于此类数据自由流动的2016/679号条例，并废除95/46/EC号指令（《一般数据保护条例》）（官方公报， 119，2016年5月4日，第1页）。

味和击键特征，目的是通过比较个人的生物识别数据和参考数据库中存储的个人生物识别数据来确定个人身份，无论个人是否同意。这不包括旨在用于生物验证，包括用于鉴别的人工智能系统，其唯一目的是确认特定自然人就是他或她声称的那个人，以及确认自然人的身份，其唯一目的是获得服务、解锁设备或安全进入场所。

(7b) 本条例中使用的生物分类概念应界定为根据生物类别数据将自然人归入特定的类别。这些特定的类别可能涉及性别、年龄、发色、眼色、纹身、行为或个性特征、语言、宗教、少数民族成员身份、性取向或政治倾向等方面。这不包括与另一项商业服务有内在联系的作为纯粹辅助功能的生物识别分类系统，也就是说，由于客观的技术原因，该功能不能在没有主要服务的情况下使用，而且对该功能的整合不是规避本条例规则的适用性的手段。例如，在线市场上使用的对面部或身体特征进行分类的过滤器可能构成此类辅助功能，因为其只能用于与主服务相关的部分，而主服务是通过允许消费者预览产品在其身上的显示效果并帮助消费者做出购买决定来销售产品。在线社交网络服务中使用的过滤器对面部或身体特征加以分类，以便用户添加或修改图片或视频，也可视为辅助功能，因为如果没有社交网络服务的主要服务，即在线分享内容，就不能使用这种过滤器。

(8) 本条例中使用的远程生物分类系统的概念应从功能上加以定义，这是一种人工智能系统，用于在自然人没有主动参与的情况下，通常是在一定距离之外，通过将一个人的生物识别数据与参考数据库中的生物识别数据进行比较来鉴别其身份，而不论所使用的生物识别数据的特定技术、程序或类型如何。这种远程生物识别系统通常用于同时感知多个人或其行为，以便在没有自然人主动参与的情况下极大地便利对自然人的识别。这不包括用于生物验证，包括用于鉴别的人工智能系统，其唯一目的是确认特定自然人就是他或她声称的那个人，以及确认自然人的身份，其唯一目的是获得服务、解锁设备或安全进入场所。这种排除的理由是，与远程生物鉴别系统相比，这类系统对自然人基本权利的影响可能较小，因为远程生物鉴别系统可用于处理许多人的生物识别数据，而无需这些人的积极参与。在“实时”系统中，生物识别数据的采集、比对和识别都是在瞬间或接近瞬间进行的，或在任何情况下都没有明显的延迟。在这方面，不应存在通过设定轻微的延迟来规避本条例关于“实时”使用有关人工智能系统的规则的空间。实时 "系统涉及使用“实时”或“近乎实时”的材料，如摄像机或其他具有类似功能的设备生成的录像片段。相比之下，“事后”系统则是生物识别数据已经得到采集，只有在延迟之后才进行比对和识别。这涉及在对有关自然人使用该系统之前已经生成的材料，如闭路电视摄像机或私人设备生成的图片或录像。

(8a) 在本条例中，情绪识别系统的概念应界定为根据自然人的生物识别数据识别或推断其情绪或意图的人工智能系统。这是指诸如快乐、悲伤、愤怒、惊讶、厌恶、尴尬、兴奋、羞愧、蔑视、满意和娱乐等情绪或意图。这不包括身体状态，如疼痛或疲劳。例如用于检测职业飞行员或司机疲劳状态以防止事故发生的系统。这也不包括仅仅检测容易察觉的表情、手势或动作，除非这是用来识别或推断情绪的。这些表情可以是基本的面部表情，如皱眉或微笑，或手势，如手、手臂或头部的动作，或者一个人的声音特征，如提高声音或低声说话。

(9) 为了本条例的目的，公众可进入场所的概念应理解为指任何数量不特定的

自然人可以进入的有形场所，而不论该场所是私有还是公有，也不论该场所可用于何种活动，如商业（如商店、餐馆、咖啡馆）、服务（如银行、专业活动、招待）、体育（如游泳池、健身房、体育场）、交通（如公共汽车、地铁和火车站、机场）、如商业（如商店、餐馆、咖啡馆）、服务业（如银行、专业活动、接待）、体育（如游泳池、健身房、体育场）、交通（如公共汽车站、地铁站、火车站、机场、交通工具）、 娱乐（如电影院、剧院、博物馆、音乐厅和会议厅）、休闲或其他（如公共道路和广场、公园、森林、游乐场）场所。如果不考虑潜在的容纳能力或安全限制，一个场所也应归类为公众可进入的场所，即使进入该场所必须满足若干预先确定的条件，如购买门票或交通工具票证、事先登记或达到一定年龄。与此相反，如果根据与公共安全或安全保障直接相关的欧盟或国家法律，或者根据对特定场所拥有相关权利的人明确表示的意思，一处场所仅限于特定和明确的自然人进入，则不应被视为公众可进入的场所。即使存在相反的迹象或情况（如禁止或限制进入的标志），仅凭进入的事实可能性（如门未上锁、栅栏门开着）并不意味着可以进入。只有相关员工和服务提供者才能进入的公司、工厂、办公室和工作场所不属于公众可进入场所。公众可进入场所不应包括监狱或边境管制。其他一些区域可能既包括不对公众开放的区域，也包括对公众开放的区域，例如私人住宅楼的走廊，这是进入医生办公室或机场所必需的。网络空间也不包括在内，因为这不是物理空间。然而，某一空间是否对公众开放，应根据具体情况具体分析。

(9b) 为了从人工智能系统中获得最大的利益，同时保护基本权利、健康和安全，并实现民主的控制，人工智能素养应使得提供者、部署者和受影响者具备必要的概念，以便就人工智能系统做出知情的决定。这些概念可能因相关背景而异，可包括了解人工智能系统开发阶段技术要素的正确应用、使用过程中应采取的措施、解释人工智能系统输出结果的适当方式，以及对于受影响者而言，了解在人工智能协助下做出的决定将如何影响他们所需的知识。在应用本条例时，人工智能素养应为人工智能价值链中的所有相关参与者提供必要的见解，以确保适当的合规性和正确的执行。此外，广泛实施人工智能素养措施并采取适当的后续行动，可有助于改善工作条件，并最终维持联盟中值得信赖的人工智能的巩固和创新之路。欧洲人工智能委员会应支持欧盟委员会（“委员会”）推广人工智能素养工具，提高公众对使用人工智能系统的好处、风险、保障措施、权利和义务的认识和理解。委员会和成员国应与利益相关方合作，促进起草自愿行为守则，以提高从事人工智能开发、运营和使用的人员的人工智能素养。

(10) 为了确保公平的竞争环境，有效保护联盟个人的权利和自由，本条例制定的规则应以非歧视的方式适用于人工智能系统的提供者，无论是在联盟内建立还是在第三国建立，也适用于在联盟内建立的人工智能系统的部署者。

(11) 鉴于其数字化的性质，特定的人工智能系统应属于本条例的范围，即使其既没有投放市场，也没有投入使用，也没有在欧盟内使用。例如，在欧盟内设立的运营商将特定服务承包给在欧盟外设立的运营商，由人工智能系统执行某项高风险的活动，就属于这种情况。在这种情况下，欧盟以外的运营商所使用的人工智能系统可以处理在欧盟境内合法收集并从欧盟转移的数据，并向欧盟内的签约运营商提供该人工智能系统在处理过程中产生的输出结果，而无需将该人工智能系统投放到欧盟市场、投入使用或在欧盟境内使用。为防止规避本条例，并确保有效保护欧盟境内的自然人，本条例也应适用于在第三国设立的

人工智能系统的提供者和部署者，只要这些系统产生的输出结果意图在欧盟境内使用。尽管如此，考虑到现有安排以及未来与外国合作伙伴进行信息和证据交换合作的特殊需要，本条例不应适用于在国家或欧洲层面与欧盟或其成员国缔结的执法和司法合作的合作或国际协议框架内行事的第三国公共机关和国际组织，条件是该第三国或国际组织在保护个人基本权利和自由方面提供充分的保障。在相关情况下，这也可包括受第三国委托执行具体任务以支持此类执法和司法合作的实体的活动。成员国与第三国之间，或欧盟、欧洲刑警组织和其他欧盟机构与第三国和国际组织之间，通过双边方式建立了此类合作框架或协议。根据《反恐怖主义法》对执法和司法机关进行监督的主管机关应评估这些合作框架或国际协定是否包括关于保护个人基本权利和自由的适当保障措施。受援成员国机关和联盟机构、办公室以及在联盟内使用此类产出的机构仍有责任确保其使用符合联盟法律。在今后修订这些国际协定或缔结新协定时，缔约方应尽最大努力使这些协定符合本条例的要求。

(12) 本条例也应适用于作为人工智能系统提供者或部署者的联盟机构、办公室、团体和机关。

(12a) 如果或只要人工智能系统被投放市场、投入使用，或被用于军事、国防或国家安全目的，无论这些系统是否经过修改，都应被排除在本条例的适用范围之外，无论开展这些活动的是哪类实体，例如是公共实体还是私营实体。关于军事和国防目的，《欧盟条约》第4条第2款和第2章第5节所涵盖的成员国和欧盟共同防卫政策的具体情况证明这种排除是合理的，这些具体情况受国际公法的管辖，因此，国际公法是在军事和国防活动中使用致命武力和其他人工智能系统的更适当的法律框架。至于国家安全目的，将其排除在外的理由是，根据《欧盟条约》第4条第2节，国家安全仍是成员国的专属职责，而且国家安全活动的具体性质和业务需要以及适用于这些活动的具体国家规则也是如此。尽管如此，如果为军事、国防或国家安全目的而开发、投放市场、投入使用或使用的人工智能系统在这些目的之外临时或永久地用于其他目的（例如民用或人道主义目的、执法或公共安全目的），这样的系统将属于本条例的范围。

(12c) 本条例应支持创新，尊重科学自由，而不应损害研发活动。因此，有必要将专门为科学研究和开发目的而开发和投入使用的人工智能系统和模型排除在其范围之外。此外，有必要确保该条例不会影响人工智能系统或模型在投放市场或投入使用之前的科学研发活动。至于以产品为导向的人工智能系统或模型的研究、测试和开发活动，在这些系统和模型投入使用或投放市场之前，本条例的规定也不应适用。但这并不影响属于本条例适用范围的人工智能系统因研发活动而投放市场或投入使用时遵守本条例的义务，也不影响有关监管沙盒和在真实世界条件下进行测试的规定的适用。此外，在不影响上述关于专门为科学研究和开发目的而开发和投入使用的人工智能系统的前提下，可能用于开展任何研究和开发活动的任何其他人工智能系统仍应遵守本条例的规定。在任何情况下，任何研发活动都应按照公认的科学研究道德和专业标准进行，并应根据适用的欧盟法律进行。

(14) 为了对人工智能系统采用一套成比例和有效的具有约束力的规则，应遵循明确界定的基于风险的方法。这种方法应根据人工智能系统可能产生的风险的强度和范围来调整此类规则的类型和内容。因此，有必要禁止某些不可接受的人工智能实践，规定高风险人工智能系统的要求和相关运营商的义务，并规定某些人工智能系统的透明度义务。

(14a) 虽然基于风险的方法是一套成比例和有效的约束性规则的基础，但重要的是要回顾委员会任命的独立人工智能高级别专家组制定的《值得信赖的人工智能的伦理准则》。在这些准则中，高级别专家组制定了七项不具约束力的人工智能伦理原则，这些原则应有助于确保人工智能是值得信赖的、符合伦理道德的。这七项原则包括：人类主体和监督；技术稳健性和安全性；隐私和数据治理；透明度；多样性、非歧视和公平；社会和环境福祉以及问责制。在不影响本条例和任何其他适用的联盟法律的法律约束力要求的前提下，这些指南有助于设计一个符合《宪章》和作为联盟基础的价值观的连贯、可信和以人为本的人工智能。根据独立人工智能高级别专家组的指南，人类主体和监督意味着人工智能系统的开发和使用是为人服务的工具，尊重人的尊严和个人自主权，其运行方式可由人类进行适当控制和监督。技术稳健性和安全性是指，开发和使用人工智能系统的方式应能在出现问题时保持稳健，并能抵御试图改变人工智能系统的使用或性能的行为，从而允许第三方非法使用，并最大限度地减少意外伤害。隐私和数据管理是指人工智能系统的开发和使用符合现有的隐私和数据保护规则，同时处理的数据在质量和完整性方面符合高标准。透明度是指人工智能系统的开发和使用方式应允许适当的可追溯性和可解释性，同时让人类意识到他们与人工智能系统进行了交流或互动，并适当告知部署者该人工智能系统的能力和局限性，以及受影响者的权利。多样性、非歧视和公平性是指人工智能系统的开发和使用方式应包括不同的参与者，并促进平等获取、性别平等和文化多样性，同时避免联盟或国家法律所禁止的歧视性影响和不公平偏见。社会和环境福祉是指以可持续和环保的方式开发和使用人工智能系统，并使全人类受益，同时监测和评估对个人、社会和民主的长期影响。在可能的情况下，这些原则的适用应转化为人工智能模型的设计和使用。在任何情况下，这些原则都应作为根据本条例起草行为守则的基础。鼓励所有利益相关者，包括产业界、学术界、公民社会和标准化组织，在制定自愿性最佳实践和标准时酌情考虑这些伦理原则。

(15) 除了人工智能的许多有益用途外，该技术也可能被滥用，并为操纵、剥削和社会控制实践提供新颖且强大的工具。这种实践特别有害，具有滥用性质，应予以禁止，因为这种实践违背了欧盟尊重人的尊严、自由、平等、民主和法治的价值观以及欧盟的基本权利，包括不受歧视的权利、数据保护和隐私权以及儿童权利。

(16) 人工智能的操纵技术可被用来劝说人们做出不想要的行为，或通过诱导其做出决定来加以欺骗，从而颠覆和损害他们的自主、决策和自由选择。在市场上投放、投入使用或使用特定的人工智能系统，其目的或效果是实质性地扭曲人的行为，从而可能造成重大伤害，特别是对身体、心理健康或经济利益产生足够重要的不利影响，这是特别危险的，因此应予禁止。这类人工智能系统采用潜意识的成分，例如人们无法感知的音频、图像、视频刺激，因为这些刺激超出了人的感知范围，或者采用其他操纵或欺骗技术，以人们无法意识到的方式颠覆或损害人的自主、决策或自由选择，或者即使意识到了，人们仍然被欺骗，或者无法控制或抵制。例如，脑机界面或虚拟现实就可能促进这种情况的发生，因其允许对呈现给人的刺激进行更大程度的控制，只要这些刺激可能会以明显有害的方式实质性地扭曲人的行为。此外，人工智能系统还可能以其他方式利用个人或特定群体由于年龄、2019/882号指令所指的残疾或特定的社会或经济状况，相应社会或经济状况可能使得这些人更容易受到剥削，例如生活

在极端贫困中的人、少数民族或宗教少数群体。此类人工智能系统可被投放市场、投入使用或使用，其目的或效果是实质性地扭曲个人的行为，并对该人或其他个人或群体造成，或者有合理可能性地造成重大的危害，包括可能长期累积的危害，因此应予禁止。如果扭曲行为是人工智能系统之外的因素造成的，而这些因素又不在提供者或部署者的控制范围之内，也就是说，人工智能系统的提供者或部署者可能无法合理地预见和缓解这些因素，则可能无法推定有扭曲行为的意图。在任何情况下，提供者或部署者不一定要具备造成重大伤害的意图，只要这种伤害是由人工智能操纵或剥削行为造成的。对此类人工智能行为的禁止是对2005/29/EC号指令所载规定的补充，特别是在任何情况下都禁止对消费者造成经济或金融损害的不公平商业行为，无论这些行为是通过人工智能系统还是其他方式实施的。本条例对操纵性和剥削性实践的禁止不应影响医疗方面的合法实践，如精神疾病的心理治疗或身体康复，如果这些实践是根据适用的法律和医疗标准进行的，例如得到个人或其法定代表人的明确同意。此外，符合适用法律的常见的合法商业行为，如广告领域的行为，本身不应被视为构成有害的人工智能操纵行为。

(16a) 应禁止基于个人生物识别数据（如个人的脸部或指纹）的生物识别分类系统来推断或推断个人的政治观点、工会成员身份、宗教或哲学信仰、种族、性生活或性取向。这项禁令不包括根据生物识别数据对按照欧盟或国家法律获取的生物识别数据集进行合法标记、过滤或分类，例如根据头发颜色或眼睛颜色对图像进行分类，这可能用于执法领域。

(17) 由公共或私人行为者为自然人提供社会评分的人工智能系统可能导致歧视性结果和排斥某些群体。这类人工智能系统可能会侵犯尊严和不受歧视的权利以及平等和公正的价值观。这类系统根据与自然人在多种场景中的社会行为有关的多个数据点或者已知、推断或预测的特定时期的个人或个性特征，对自然人或其群体进行评估或分类。从此类人工智能系统中获得的社会评分可能会导致自然人或其整个群体在社会环境中受到有害或不利待遇，而这些环境与最初生成或收集数据的场景无关，或者导致与其社会行为的严重程度不成比例或不合理的不利待遇。因此，应禁止人工智能系统采用这种不可接受的评分方法，导致这种有害或不利的结果。这一禁令不应影响自然人根据国家和欧盟法律为特定目的而进行的合法的评估行为。

(18) 为执法目的使用人工智能系统在公共场所对自然人进行“实时”远程生物鉴别，对有关个人的权利和自由具有特别的侵扰性，因为这类系统可能影响大部分人的私生活，使人产生始终受到监视的感觉，并间接地妨碍行使集会自由和行使其他基本权利。用于对自然人进行远程生物识别的人工智能系统在技术上的不准确性可能会导致存在偏差的结果并产生歧视性影响。在涉及年龄、民族、种族、性别或残疾时，这一点尤为重要。此外，使用这种“实时”运行的系统，其影响具备即时性，进一步检查或纠正的机会有限，给执法活动所涉及的人的权利和自由带来了更大的风险。

(19) 因此，应禁止为执法目的使用这些系统，除非在详尽列出和严格界定的情况下，使用这些系统对实现重大公共利益是严格必要的，其重要压倒了风险。这些情况包括：寻找特定犯罪受害者，包括失踪人员；自然人的生命或人身安全受到特定的威胁或者受到恐怖袭击；确定附件二a所述刑事犯罪的犯罪人或嫌疑人的位置或身份，条件是这些刑事犯罪在有关成员国应受到监禁判决或拘留令的惩罚，最长期限至少为四年，而且该成员国的法律对此有明确规定。根据

国家法律，这种监禁判决或拘留令的门槛有助于确保罪行的严重程度足以证明使用“实时”远程生物鉴别系统是合理的。此外，附件二a中提到的刑事犯罪清单是以理事会2002/584/JHA号框架决定[9]中列出的32种刑事犯罪为基础的，同时考虑到在实践中特定的刑事犯罪可能比其他刑事犯罪干系更大，在实际追查所列不同刑事罪行的犯罪人或嫌疑人的定位或识别工作中，采用“实时”远程生物鉴别技术在可预见的程度上应是必要且成比例的。
根据2008/114/EC号指令第2条第a点的定义，关键基础设施的严重破坏也可能导致对自然人的生命或人身安全的迫在眉睫的威胁，包括对向居民提供基本供应或行使国家核心职能造成严重损害。
此外，本条例应保留执法、边境管制、移民或庇护机关根据联盟和国家法律规定的身份检查条件，在当事人在场的情况下进行身份检查的能力。特别是，执法、边境管制、移民或庇护机关应能根据欧盟或国家法律使用信息系统来识别在身份检查期间拒绝被识别或无法说明或证明其身份的人，而无需根据本条例事先获得授权。例如，这可能是一个涉及犯罪、不愿或因事故或健康状况而无法向执法机关透露其身份的人。
(20) 为了确保以负责任和成比例的方式使用这些系统，还必须规定，在详尽无遗地列出和狭义界定的每一种情况下，都应考虑到特定的因素，特别是引起请求使用的情况的性质和使用对所有有关人员的权利和自由的后果，以及使用所提供的保障和条件。此外，在公共场所为执法目的使用“实时”远程生物鉴别系统，只能用于确认特定目标个人的身份，并应仅限于在时间、地理和个人范围方面严格必要的情况，尤其应考虑到有关威胁、受害者或犯罪者的证据或迹象。在公共场所使用“实时”远程生物识别系统，只有在执法机关完成了基本权利影响评估，并在本条例规定的数据库中登记了该系统的情况下，方可授权使用。人员的所引数据库应适合上述每种情况下的每种用例。
(21) 在公共场所为执法目的使用“实时”远程生物鉴别系统，每次使用都应得到司法机关或其决定对成员国具有约束力的独立行政机关的明确和具体授权。这种授权原则上应在使用该系统识别某人或某些人之前获得。在有正当理由的紧急情况下，即在需要使用有关系统，因而实际上和客观上不可能在开始使用之前获得授权的情况下，这一规则应允许例外。在这种紧急情况下，使用应限制在严格必要的最低限度，并受制于适当的保障措施和条件，这些措施和条件由国家法律确定，并由执法机关本身在每个紧急使用的个案中具体规定。此外，在这种情况下，执法机关应在提出申请的同时，说明未能及早提出申请的原因，不得无故拖延，最迟应在24小时内提出申请。如果这种授权被拒绝，则应立即停止使用与该授权有关的实时生物鉴别系统，并应弃置和删除与这种使用有关的所有数据。这些数据包括人工智能系统在使用过程中直接获得的输入数据，以及与该授权相关的使用结果和输出。这不应包括根据其他国家或欧盟法律合法获取的输入数据。在任何情况下，不得仅根据远程生物识别系统的输出结果做出对个人产生不利法律影响的决定。
(21a) 为了按照本条例以及国家规则中规定的要求执行任务，应将“实时生物识别系统”的每次的使用情况通知有关国家市场监督管理机关和国家数据保护机构。已收到通知的国家市场监督管理机关和国家数据保护机关应向欧盟委员

[9] 理事会2002年6月13日关于欧洲逮捕令和成员国之间的移交程序的2002/584/JHA号框架决定（官方公报 190，2002年7月18日，第1页）。

会提交关于“实时生物识别系统”使用情况的年度报告。
(22) 此外，应当在本条例规定的详尽框架内，规定只有在有关成员国决定在其国内法的详细规则中明确规定可以授权在其领土内使用这类系统，才可能根据本条例在其领土内使用。因此，根据本条例，成员国仍可完全不对这种可能性加以规定，或仅就本条例所确定的可证明有理由授权使用的特定目标规定这种可能性。这些国家规则最迟应在其通过后30天内通知欧盟委员会。
(23) 为执法目的而使用人工智能系统对公共场所的自然人进行“实时”远程生物识别，必然涉及生物识别数据的处理。本条例基于《欧洲联盟运作条约》第16条禁止此类使用的规则，除特定的例外情况之外，应作为特别法适用于2016/680号指令第10条所载的生物识别数据处理规则，从而以详尽的方式规范此类使用和所涉及的生物识别数据处理。因此，此类使用和处理只能在符合本条例规定的框架内进行，而不能在该框架之外，由主管机关以执法为目的，根据2016/680 号指令第10条所列的理由使用此类系统并处理相关数据。在此背景下，本条例无意为根据2016/680号指令第8条处理个人数据提供合法性基础。然而，在公共场所为执法以外的目的使用“实时”远程生物识别系统，包括由主管机关使用，不应包括在本条例规定的有关为执法目的使用此类系统的具体框架内。因此，为执法以外的目的使用此类系统不应受本条例规定的授权要求和可能使本条例生效的国内法适用细则的限制。
(24) 在使用人工智能系统进行生物识别时涉及的生物识别数据和其他个人数据的任何处理，除与本条例规定的为执法目的在公共场所使用“实时”远程生物识别系统有关外，应继续遵守2016/680号指令第10条规定的所有要求。对于执法以外的目的，2016/679号条例第9条第1款和2018/1725号条例第10条第1款禁止处理生物识别数据，但这些条款规定的有限的例外情况除外。在适用2016/679号条例第9条第1款时，远程生物特征识别用于执法以外的目的的已经落入国家数据保护机关的禁止决定之下。
(25) 根据《欧洲联盟条约》和《欧洲联盟运作条约》所附《关于联合王国和爱尔兰在自由、安全和司法领域的立场的第21号议定书》第6a条，爱尔兰不受第5条第1款第d、2、3、3a、4和5项、第5条第1款第ba项中规定的规则的约束，只要该条适用于在警察合作和刑事司法合作领域的活动中使用生物识别分类系统、第5条第1款第da项适用于该条款和根据《欧盟运作条约》第16条通过的本条例第 29条第6a款所涵盖的人工智能系统的使用，涉及成员国在开展《欧盟运作条约》第三部分第5节第四章或第五章范围内的活动时对个人数据的处理，其中爱尔兰不受对遵守根据《欧洲联盟运作条约》第16条制定的规定的刑事事项司法合作或警务合作形式规则的要求的约束。
(26a) 根据无罪推定原则，欧盟的自然人应始终根据其实际行为进行判断。在没有基于客观可核实事实的合理怀疑自然人参与犯罪活动且未经人工评估的情况下，绝不应仅根据其画像、个性特征或特点，如国籍、出生地、居住地、子女人数、债务、汽车类型等，对自然人的行为进行人工智能的预测判断。因此，应禁止对自然人进行风险评估，以评估其犯罪的风险，应禁止根据对自然人的画像或对其个性特征和特点的评估来预测实际或潜在刑事犯罪的发生。在任何情况下，这一禁止都不涉及也不触及并非基于个人画像或者个性特征或特点的风险分析，例如使用风险分析的人工智能系统根据可疑交易评估企业的金融欺诈风险，或使用风险分析工具预测海关机关将麻醉品或非法货物本地化的可能性，例如根据已知的贩运路线而预测。

(26b) 应禁止将人工智能系统投放市场、为这一特定目的投入使用或使用，这些系统通过从互联网或闭路电视录像中无针对性地获取面部图像来创建或扩大面部识别数据库，因为这种实践会增加大规模监控的感觉，并可能导致严重侵犯基本权利，包括隐私权。
(26c) 人们对旨在识别或推断情绪的人工智能系统的科学依据表示严重的关切，特别是在不同文化和不同情况下，甚至在同一个人身上，情绪的表达都有很大差异。这类系统的主要缺点包括可靠性有限、缺乏特异性和通用性有限。因此，根据生物识别数据识别或推断自然人情绪或意图的人工智能系统可能导致歧视性结果，并可能侵犯相关人员的权利和自由。考虑到工作或教育方面的权力不平衡，再加上这些系统的侵扰性，这些系统可能会导致特定自然人或整个自然人群体受到有害或不利的待遇。因此，应禁止将旨在用于检测个人在工作场所和教育相关情况下的情绪状态的人工智能系统投放市场、投入使用或使用。这一禁令不应包括严格出于医疗或安全原因而投放市场的人工智能系统，如用于治疗的系统。
(26d) 数据保护法、非歧视法、消费者保护法和竞争法等欧盟立法所禁止的实践不受本条例影响。
(27) 高风险人工智能系统只有在符合特定强制性要求的情况下才能进入欧盟市场、投入使用或使用。这些要求应确保在欧盟提供的高风险人工智能系统或其产出在欧盟使用的高风险人工智能系统不会对欧盟法律承认和保护的重要欧盟公共利益构成不可接受的风险。根据新立法框架方法，正如欧盟委员会关于实施欧盟产品规则的2022年《蓝皮书指南》的通知（C/2022/3637）所阐明的，一般的规则是，同一产品需要考虑欧盟的若干立法，如关于医疗器械的2017/745号条例和关于体外诊断器械的2017/746号条例或关于机械的2006/42/EC号指令，因为只有当产品符合所有适用的欧盟统一立法时，才能提供或投入使用。为确保一致性并避免不必要的行政负担或成本，对于包含一个或多个高风险人工智能系统的产品，本法规要求以及附件IIA部分所列欧盟统一立法的要求适用于该产品，其提供者应灵地做出运营操作决定，以最佳方式确保包含一个或多个人工智能系统的产品符合欧盟统一立法的所有适用要求。识别为高风险的人工智能系统应仅限于那些对欧盟内人员的健康、安全和基本权利有重大有害影响的系统，这种限制应最大限度地减少对国际贸易的任何潜在限制，如有。
(28) 人工智能系统可能对人的健康和安全产生不利影响，特别是当这些系统作为产品的安全组件时。欧盟统一立法的目标是促进产品在内部市场的自由流动，并确保只有安全和符合要求的产品才能进入市场，与此相一致，重要的是，产品作为一个整体，其数字组件，包括人工智能系统，可能产生的安全风险应得到适当的预防和缓解。例如，越来越多的自主机器人，无论是在制造领域还是在个人协助和护理领域，都应该能够在复杂的环境中安全运行并执行其功能。同样，在对生命和健康的风险特别高的卫生部门，日益复杂的诊断系统和支持人类决策的系统应该是可靠和准确的。
(28a) 在将人工智能系统列为高风险时，人工智能系统对《宪章》所保护的基本权利造成的不利影响程度特别重要。这些权利包括人的尊严权、尊重私人和家庭生活权、保护个人数据权、言论和信息自由权、集会和结社自由权、不受歧视权、受教育权、消费者保护权、工人权利、残疾人权利、性别平等、知识产权、获得有效救济和公平审判的权利、辩护权和无罪推定权、良好管理权。除这些权利外，必须强调的是，《欧盟条约》第24条和《联合国儿童权利公

约》关于数字环境的第25号一般性意见作了进一步阐述，规定儿童享有特定地权利，这两项公约都要求考虑儿童的脆弱性，并为其福祉提供必要的保护和照顾。在评估人工智能系统可能造成的危害的严重程度时，包括在涉及人的健康和安全方面，也应考虑到《宪章》中规定并在欧盟政策中实施的受到高度的环境保护的基本权利。

(29) 至于作为产品或系统安全组件的高风险人工智能系统，或其本身属于欧洲议会和理事会300/2008号条例[10]、欧洲议会和理事会167/2013号条例[11]范围内的产品或系统、欧洲议会和欧盟理事会168/2013号条例[12]、欧洲议会和欧盟理事会2014/90/EU号指令[13]、欧洲议会和欧盟理事会2016/797号指令[14] 、欧洲议会和欧盟理事会2018/858号条例[15]、欧洲议会和欧盟理事会2018/1139号条例[16]，以及欧洲议会和欧盟理事会2019/2144号条例[17] ，宜对这些法案进行修订，以确保委员会在根据这些法案通过任何相关的未来授权法案或实施法案时，根据各部门的技术和监管的特殊性，并在不干扰现有治理、合格性评估和执行机制以及在其中建立的权威机构的情况下，考虑到本条例对高风险人工智能系统规定的强制性要求。

(30) 对于属于附件II所列的特定欧盟统一立法范围内的产品安全组件或产品本身的人工智能系统，如果有关产品根据相关欧盟统一立法在第三方合格性评定机构进行合格性评定程序，则宜根据本条例将其归类为高风险。具体而言，此类产品包括机械、玩具、电梯、用于潜在爆炸性气体环境的设备和保护系统、无线电设备、压力设备、娱乐船设备、索道装置、燃烧气体燃料的设备、医疗器械和体外诊断医疗器械。

(31) 根据本条例将人工智能系统归类为高风险并不一定意味着以人工智能系统为安全组件的产品，或作为产品的人工智能系统本身，根据适用于该产品的相关欧盟统一立法中规定的标准被视为“高风险”。欧洲议会和欧盟理事会

---

[10] 欧洲议会和理事会2008年3月11日关于民用航空安全领域共同规则的300/2008号条例，废除2320/2002号条例（官方公报， 97，2008 年 4 月 9 日，第 72 页）。

[11] 欧洲议会和理事会2013年2月5日关于农林车辆审批和市场监管的167/2013号条例（官方公报， 60，2013年3月2日，第1页）。

[12] 欧洲议会和欧盟理事会2013年1月15日关于两轮或三轮汽车和四轮车审批和市场监督的168/2013号条例（官方公报， L 60，2013年3月2日，第52页）。

[13] 欧洲议会和理事会2014年7月23日关于海洋设备的2014/90/EU号指令，废除理事会96/98/EC号指令（官方公报，257，2014年8月28日，第146页）。

[14] 欧洲议会和欧盟理事会2016年5月11日关于欧盟内部铁路系统互操作性的2016/797号指令（官方公报，138，2016年5月26日，第44页）。

[15] 欧洲议会和欧盟理事会 2018 年 5 月 30 日关于机动车辆及其挂车，以及用于此类车辆的系统、组件和独立技术单元的审批和市场监督的 2018/858 号条例，修订 715/2007 号和 595/2009 号条例，并废止 2007/46/EC 号指令（官方公报，151，2018 年 6 月 14 日，第 1 页）。

[16] 欧洲议会和理事会 2018 年 7 月 4 日关于民用航空领域共同规则和建立欧盟航空安全局的 2018/1139 号条例，并修订 2111/2005 号、1008/2008 号、996/2010 号条例、376/2014 号以及欧洲议会和理事会 2014/30/EU 号指令和 2014/53/EU 号指令，并废除欧洲议会和理事会条例 552/2004 号条例和 216/2008 号条例以及理事会 3922/91 号条例（官方公报，212，2018 年 8 月 22 日，第 1 页）。

[17] 欧洲议会和欧盟理事会 2019 年 11 月 27 日 2019/2144 号条例，关于机动车辆及其挂车，以及用于此类车辆的系统、组件和独立技术单元在一般安全和保护车内人员及易受伤害的道路使用者方面的类型批准要求，修订欧洲议会和欧盟理事会 2018/858 号条例，并废止 78/2009 号条例、欧洲议会和欧盟理事会 78/2009 号、79/2009 号和 661/2009 号条例，以及欧盟委员会 631/2009、406/2010、672/2010、1003/2010、1005/2010 号条例、1008/2010、1009/2010、19/2011、109/2011、458/2011、65/2012、130/2012、347/2012、351/2012、1230/2012 和 2015/166 号条例（官方公报，325，2019 年 12 月 16 日,第 1 页）。.

2017/745号条例[18]和欧洲议会和欧盟理事会2017/746号条例[19]就是明显的例子，其中为中等风险和高风险产品提供了第三方合格性评估。

(32) 至于独立的人工智能系统，即除开作为产品安全组件或本身就构成产品的高风险人工智能系统之外的其他系统，如果根据其预期目的，考虑到可能造成伤害的严重性及其发生的概率， 其对人的健康和安全或基本权利造成伤害的风险很高，而且其用于本条例具体规定的一些预先确定的领域，那么将其归类为高风险系统是适当的。确定这些系统所依据的方法和标准与今后修订高风险人工智能系统清单所设想的方法和标准相同，委员会应有权通过授权法案对高风险人工智能系统清单进行修订，以考虑到技术的快速发展以及人工智能系统使用方面的潜在变化。

(32a) 同样重要的是要澄清，在一些具体情况下，本条例规定的领域前提到的人工智能系统不会导致对这些领域所保护的法律利益造成重大损害的风险，因为这些系统不会对决策产生实质性影响，或不会对这些利益造成实质性损害。就本条例而言，不对决策结果产生实质性影响的人工智能系统应理解为不影响决策的实质内容，从而不影响决策结果的人工智能系统，无论是人为决策还是自动决策。如果满足以下一个或多个条件，就可以这样理解。第一个标准应该是，人工智能系统的目的是执行范围狭窄的程序性任务，例如将非结构化数据转换为结构化数据的人工智能系统、将收到的文件分类的人工智能系统或用于检测大量应用程序中重复内容的人工智能系统。这些任务的范围很窄，性质有限，只会带来有限的风险，不会因为在附件三所列的环境中使用而增加风险。第二个标准应该是，人工智能系统执行的任务旨在改进先前完成的人类活动的结果，而该活动可能与附件三所列用例的目的有关。考虑到这些特点，人工智能系统只是为人类活动提供了一个附加曾，从而降低了风险。例如，本标准适用于旨在改进先前起草的文件中所用语言的人工智能系统，例如在专业语气、学术语言风格方面，或通过使文本与某些品牌信息保持一致。第三条标准应该是人工智能系统旨在检测决策模式或偏离先前的决策模式的情况。此时风险也会有所降低，因为人工智能系统的使用是在先前完成的人工评估之后进行的，人工智能系统不是要在没有经过适当的人工审查的情况下替代或者影响人类评估。例如，这类人工智能系统可以在给某位教师打分时，事后检查该教师是否偏离了打分模式，以发现潜在的不一致或异常。第四个标准应该是，人工智能系统旨在执行的任务只是与附件三所列用例目的相关的评估的准备工作，从而使系统输出的可能的影响非常小，不会对接下来的评估造成风险。例如，这一标准涵盖了文件处理的智能解决方案，其中包括索引、搜索、文本和语音处理或将数据链接到其他数据源等各种功能，或用于翻译初始文件的人工智能系统。在任何情况下，如果附件三中提到的人工智能系统意味着2016/679号条例第4条第4款和2016/680号指令第3条第4款以及2018/1725号条例第3条第5款所指的画像，则应认为该人工智能系统对自然人的健康、安全或基本权利构成明显的损害风险。为确保可追溯性和透明度，根据上述标准认为附件三所述人工智能系统不属于高风险的提供者应在该系统投放市场或投入使用前起草评估文件，并应根据要求向国家主管机关提供该文件。此类提供者有义务在根据本条

[18] 欧洲议会和理事会2017年4月5日关于医疗器械的2017/745 号条例，修订2001/83/EC号指令、178/2002号条例和1223/2009 号条例，并废除90/385/EEC号和93/42/EEC号指令（官方公报，117，2017年5月5日，第1页）。

[19] 欧洲议会和欧盟理事会 2017 年 4 月 5 日关于体外诊断医疗器械的 2017/746 号条例，废除 98/79/EC 号指令和 2010/227/EU 号决定（官方公报，117，2017 年 5 月 5 日，第 176 页）。

例建立的欧盟数据库中登记该系统。为了进一步指导实际执行附件三所述人工智能系统在特殊情况下不属于高风险的标准，委员会应在与人工智能委员会协商后，提供具体的实际执行准则，并附上人工智能系统高风险和非高风险使用案例的全面的实例清单。

(33a) 由于生物识别数据是一类特殊的敏感个人数据，因此将生物识别系统的几种关键用例归类为高风险用例是适当的，只要其使用是欧盟和国家相关法律所允许的。

用于对自然人进行远程生物识别的人工智能系统在技术上的不准确性可能会导致有偏差的结果并产生歧视性影响。这在涉及年龄、民族、种族、性别或残疾时尤其如此。因此，鉴于远程生物识别系统所带来的风险，应将其归类为高风险系统。这不包括旨在用于生物验证， 包括鉴别的人工智能系统，其唯一目的是确认特定自然人就是他或她声称的那个人，以及确认自然人的身份，其唯一目的是获得服务、解锁设备或安全进入场所。

此外，意图用于根据基于生物识别数据的受2016/679号条例第9条第1款保护的敏感属性或特征进行生物分类的人工智能系统，只要本条例未加以禁止，以及本条例未禁止的情感识别系统，应被归类为高风险系统。仅用于网络安全和个人数据保护措施的生物识别系统不应被视为高风险系统。

(34) 关于重要基础设施的管理和运作，将《关于重要实体、道路交通和供水、供气、供热和供电的韧性的指令》附件一第8点所列的意图用作重要数字基础设施管理和运作的安全组件的人工智能系统列为高风险系统是适当的，因为这些系统的故障或失灵可能会危及大规模人员的生命和健康， 并导致社会和经济活动的正常进行受到明显干扰。关键基础设施，包括关键数字基础设施的安全组件是用来直接保护关键基础设施的物理完整性或人员和财产的健康与安全的系统，但并非系统运行所必需。这些组件的故障或失灵可能直接导致重要基础设施的物理完整性受到威胁，从而危及人员和财产的健康与安全。仅用于网络安全目的的组件不应被视为安全组件。此类关键基础设施的安全组件的例子可包括云计算中心的水压监测系统或火警控制系统。

(35) 在教育领域部署人工智能系统，对于促进高质量的数字教育和培训，让所有学习者和教师获得并分享必要的数字技能和能力，包括媒体素养和批判性思维，从而积极参与经济、社会和民主进程非常重要。然而，在教育或职业培训中使用的人工智能系统，尤其是用于确定入学或录取、将人员分配到各级教育和职业培训机构或计划、评估个人的学习成果、评估个人的适当教育水平并对个人将接受或能够接受的教育和培训水平产生实质性影响，或者用于监测和检测学生在考试中的违纪行为的人工智能系统，应归类为高风险人工智能系统，因为其可能决定一个人一生的教育和职业生涯，从而影响其确保生计的能力。如果设计和使用不当，这些系统可能具有特别的侵扰性，并可能侵犯受教育和培训的权利以及不受歧视的权利，并使历史上的歧视模式永久化，例如针对妇女、特定年龄群体、残疾人或特定的种族或民族血统或性取向的人的歧视。

(36) 在就业、工人管理和自营职业中使用的人工智能系统，特别是用于招聘和选拔人员，用于做出影响工作合同关系晋升和终止的决定，用于根据个人行为、个人特征或特点分配任务，用于监测或评估工作合同关系中的人员，也应被列为高风险，因为这些系统可能会对这些人的未来职业前景、生计和工人权利产生重大影响。与工作相关的合同关系应通过委员会2021年的工作计划中提及的平台，让雇员和提供服务的人员切实参与其中。在与工作相关的合同关系

中，在整个招聘过程中，以及在对人员的评估、晋升或留用过程中，此类系统可能会延续历史上的歧视模式，例如针对妇女、特定年龄群体、残疾人或特定的种族或民族血统或性取向的人的歧视。用于监测这些个人的表现和行为的人工智能系统也可能损害他们的数据保护和隐私的基本权利。

(37) 另一个值得特别考虑使用人工智能系统的领域是获得和享受特定的必要的私人和公共服务和福利，这是人们充分参与社会或提高生活水平所必需的。特别是，申请或接受公共机关提供的基本公共援助福利和服务，即医疗保健服务、社会保障福利、在生育、疾病、工伤事故、依赖或年老和失业情况下提供的社会保护以及社会和住房援助的自然人，通常依赖于这些福利和服务，相对于负有权责的机关来说处于弱势地位。如果机关使用人工智能系统来决定是否应给予、拒绝、减少、取消或收回这些福利和服务，包括受益人是否合法享有这些福利或服务，这些系统可能会对人们的生计产生重大影响，并可能侵犯他们的基本权利，如社会保护权、不受歧视权、人的尊严权或有效补救权，因此应被列为高风险系统。尽管如此，本条例不应妨碍公共行政部门开发和使用创新方法，因为更广泛地使用合规和安全的人工智能系统将使公共行政部门受益，前提是这些系统不会给法人和自然人带来高风险。

此外，用于评估自然人的信用分数或信用度的人工智能系统应被归类为高风险人工智能系统，因为它们决定了这些人获得金融资源或住房、电力和电信服务等基本服务的机会。用于此目的的人工智能系统可能会导致对个人或群体的歧视，并延续历史上的歧视模式，例如基于种族或民族血统、性别、残疾、年龄、性取向的歧视，或造成新形式的歧视性影响。然而，根据本条例，欧盟法律规定的用于检测提供金融服务过程中的欺诈行为以及用于计算信贷机构和保险企业资本要求的审慎目的的人工智能系统不应被视为高风险系统。此外，用于自然人健康和人寿保险风险评估和定价的人工智能系统也会对人们的生活产生重大影响，如果设计、开发和使用不当，可能会侵犯他们的基本权利，并可能对人们的生活和健康造成严重后果，包括金融排斥和歧视。最后，用于对自然人的紧急呼叫进行评估和分类的人工智能系统，或用于调度或确定优先调度紧急第一反应服务的人工智能系统，包括警察、消防员和医疗援助，以及紧急医疗保健病人分流系统，也应归类为高风险，因为它们是在非常危急的情况下对人的生命和健康及其财产做出决定。

(38) 鉴于执法机关的作用和责任，执法机关涉及人工智能系统的特定用途的行动具有很大程度的权力不平衡特点，可能导致监视、逮捕或剥夺自然人的自由，以及对《宪章》保障的基本权利的其他不利影响。特别是，如果人工智能系统没有经过高质量数据的训练，在性能、准确性或稳健性方面没有达到足够的要求，或者在投放市场或以其他方式投入使用之前没有经过适当的设计和测试，这些系统可能会以歧视性或其他不正确或不公正的方式将人筛选出来。此外，重要的程序性基本权利，如获得有效救济和公正审判的权利，以及辩护权和无罪推定的行使，可能会受到阻碍，特别是在此类人工智能系统不够透明、可解释和有记录的情况下。因此，在相关欧盟和国家法律允许使用的范围内，将一些意图用于执法领域的人工智能系统归类为高风险系统是适当的，因为在执法领域，准确性、可靠性和透明度对于避免不利影响、保持公众信任以及确保可问责性和有效救济尤为重要。鉴于有关活动的性质和相关风险，这些高风险人工智能系统应特别包括意图由执法机关或代表执法机关或由联盟机构、办公室或支持执法机关的机构用于评估自然人成为刑事犯罪受害者的风险的人工

智能系统，如测谎仪和类似工具、在调查或起诉刑事犯罪的过程中，用于评估证据的可靠性，以及在本条例未禁止的范围内，用于评估自然人犯罪或再犯罪的风险，而不仅仅是基于对自然人的特征分析，或基于对自然人或群体的个性特征或以往犯罪行为的评估，用于侦查、调查或起诉刑事犯罪过程中的特征分析。专门用于税务和海关机关行政程序的人工智能系统，以及根据欧盟反洗钱立法执行行政任务、分析信息的金融情报单位使用的人工智能系统，不应被归类为执法机关为预防、侦查、调查和起诉刑事犯罪而使用的高风险人工智能系统。执法部门和机关使用人工智能工具不应成为不平等或排斥的因素。不应忽视使用人工智能工具对嫌疑人辩护权的影响，特别是难以获得关于这些系统运作的有意义信息，以及因此难以在法庭上质疑其结果，尤其是被调查的个人。

(39) 在移民、庇护和边境管制管理中使用的人工智能系统影响到的人往往处于特 别弱势的地位，他们依赖于主管公共机关的行动结果。因此，在这些情况下使用的人工智能系统的准确性、非歧视性和透明度对于保证尊重受影响者的基本权利，特别是他们的自由行动权、不受歧视权、私人生活和个人数据受保护权、受国际保护权和得到良好管理权尤为重要。因此，在欧盟和各国相关法律允许使用的范围内，将旨在由主管公共机关或代表主管 公共机关或负责移民、庇护和边境管制管理领域任务的欧盟机构、办公室或机关使用 的人工智能系统归类为高风险系统是适当的，如测谎仪和类似工具，用于评估进入成员国领土或申请签证或庇护的自然人所构成的特定风险、协助主管公共机关审查庇护、签证和居留许可申请及相关投诉，包括对证据可靠性的相关评估，目的是确定申请身份的自然人的资格，以便在移民、庇护和边境管制管理方面发现、识别或辨认自然人，但旅行证件除外。本条例涵盖的移民、庇护和边境控制管理领域的人工智能系统应符合欧洲议会和欧盟理事会2013/32/EU号指令[20]、欧洲议会和欧盟理事会810/2009号条例[21]以及其他相关立法规定的相关程序要求。在移民、庇护和边境控制管理中使用人工智能系统，在任何情况下都不应被成员国或联盟机构、机关或团体用作规避其根据经1967年1月31日议定书修正的1951年7月28日《关于难民地位的公约》所承担的国际义务的手段，也不应被用于以任何方式违反不遣返原则，或剥夺进入联盟领土的安全和有效的合法途径，包括获得国际保护的权利。

(40) 考虑到特定用于司法和民主进程的人工智能系统对民主、法治、个人自由以 及获得有效救济和公平审判的权利可能产生的重大影响，应将其归类为高风险系统。特别是，为了应对潜在的偏见、错误和不透明的风险，应将旨在由司法机关或代表司法机关使用的人工智能系统定为高风险系统，以协助司法机关研究和解释事实和法律，并将法律适用于一系列具体事实。当替代性争议解决程序的结果对当事方产生法律效力时，拟由替代性争议解决机构用于上述目的的人工智能系统也应被视为高风险系统。使用人工智能工具可以支持法官的决策权或司法独立，但不应取而代之，因为最终决策必须仍然是人类驱动的活动和决定。然而，这种限定不应延伸到纯粹用于辅助性行政活动的人工智能系统，这些活动并不影响个案中的实际司法行政，如司法判决、文件或数据的匿

[20] 欧洲议会和欧盟理事会2013年6月26日关于授予和撤销国际保护的共同程序的2013/32/EU号指令（官方公报，180，2013年6月29日，第60页）。

[21] 欧洲议会和理事会2009年7月13日810/2009号条例制定了《共同体签证法》（官方公报，243，2009年9月15日，第1 、页）。

名化或假名化，人员之间的沟通，行政任务等。
(40a) 在不影响关于政治广告透明度和针对性的第xxx号条例规定的规则的情况下，为应对《宪章》第39条规定的投票权受到不当外部干预的风险，以及对民主和法治产生不利影响的风险、旨在用于影响选举或全民投票结果或自然人在选举或全民投票中的投票行为的人工智能系统应被归类为高风险人工智能系统，但自然人不直接接触其输出结果的人工智能系统除外，例如从行政和后勤角度组织、优化和结构化政治运动的工具。
(41) 根据本条例，人工智能系统被归类为高风险人工智能系统这一事实不应被解释为表明，根据其他联盟法律或与联盟法律相容的国家法律，如关于保护个人数据、使用测谎仪和类似工具或其他系统检测自然人情绪状态的法律，使用该系统是合法的。任何此类使用均应完全按照《宪章》以及适用的欧盟次级法律和国家法律的要求继续进行。除非本条例另有明确规定，否则本条例不应被理解为提供处理个人数据（包括相关的特殊类别个人数据）的合法性基础。
(42) 为降低投放市场或投入使用的高风险人工智能系统的风险，并确保高水平的可信度，特定的强制性要求应适用于高风险人工智能系统，同时考虑到人工智能系统的预期目的和使用环境，并根据提供者建立的风险管理系统。提供者为遵守本条例的强制性要求而采取的措施应考虑到普遍认可的人工智能技术水平，并与本条例的目标成比例且有效。按照欧盟委员会关于实施欧盟产品规则2022年《蓝皮书指南》的通知（C/2022/3637）中阐明的“新立法框架”的方法，一般规则是，一个产品可能需要考虑多个欧盟立法，因为只有当产品符合所有适用的欧盟统一立法时，才能提供或投入使用。本条例的要求所涉及的人工智能系统的危险与现有的欧盟协调法案涉及不同的方面，因此本条例的要求将对现有的欧盟协调法案进行补充。例如，包含人工智能系统的机械或医疗设备产品可能会带来相关欧盟协调法规中规定的基本健康和安全要求未涉及的风险，因为该部门法规不涉及人工智能系统特有的风险。这就要求同时适用不同的法律法规，并对其进行补充。为确保一致性并避免不必要的行政负担或成本，对于包含一个或多个高风险人工智能系统的产品（本条例的要求以及附件二A部分所列欧盟统一立法的要求适用于该产品），其提供者应在运营决策方面具有灵活性，以最佳方式确保包含一个或多个人工智能系统的产品符合欧盟统一立法的所有适用要求。例如，这种灵活性可能意味着提供者决定将本条例要求的部分必要测试和报告流程、信息和文件整合到附件二A部分所列现有欧盟统一立法要求的现有文件和程序中。
(42a) 风险管理系统应包括一个持续、反复的过程，在高风险人工智能系统的整个生命周期中进行规划和运行。这一过程应旨在确定和减轻人工智能系统对健康、安全和基本权利的相关风险。应定期对风险管理系统进行审查和更新，以确保其持续有效性，并对根据本条例做出的任何重大决定和采取的行动进行说明和记录。这一过程应确保提供者根据人工智能系统的预期目的和可合理预见的滥用情况，包括人工智能系统与其运行环境之间的相互作用可能产生的风险，识别风险或不利影响，并针对已知和可合理预见的人工智能系统对健康、安全和基本权利的风险实施缓解措施。风险管理系统应根据人工智能的最新技术采取最适当的风险管理措施。在确定最合适的风险管理措施时，提供者应记录和解释所做的选择，并在相关时让专家和外部利益相关者参与进来。在确定可合理预见的对高风险人工智能系统的误用时，提供者应涵盖人工智能系统的用途，这些用途虽然不直接包括在预期目的和使用说明中，但根据特定人工智

能系统的具体特点和使用情况，可合理预期会由容易预测的人类行为导致。任何与高风险人工智能系统按照其预期目的使用或在可合理预见的滥用条件下使用有关的已知或可预见情况，可能导致健康和安全风险或基本权利风险，都应包括在提供者提供的使用说明中。这是为了确保部署者在使用高风险人工智能系统时了解并考虑到这些风险。根据本条例确定和实施针对可预见滥用的风险缓解措施，不应要求提供者针对高风险人工智能系统采取具体的额外培训措施来解决这些问题。但鼓励提供者在必要和适当的情况下，考虑采取这些额外的培训措施，以减少合理的可预见的误用。

(43) 在风险管理、所使用数据集的质量和相关性、技术文件和记录保存、透明度和向部署者提供信息、人工监督、稳健性、准确性和网络安全方面，应对高风险人工智能系统提出要求。这些要求是有效降低健康、安全和基本权利风险所必需的，而且没有其他贸易限制性较小的措施可以合理利用，从而避免对贸易造成不合理的限制。

(44) 高质量数据和获取高质量数据在提供结构和确保许多人工智能系统的性能方面发挥着至关重要的作用，特别是在使用涉及模型训练的技术时，目的是确保高风险人工智能系统按预期安全运行，并且不会成为欧盟法律禁止的歧视来源。用于训练、验证和测试的高质量数据集需要实施适当的数据治理和管理实践。用于培训、验证和测试的数据集（包括标签）应具有相关性和足够的代表性，并在最大程度上不存在错误，而且从系统的预期目的来看应是完整的。为便于遵守欧盟数据保护法，如2016/679 号条例，数据治理和管理实践应包括：就个人数据而言，数据收集的原始目的应当透明；数据集还应具有适当的统计属性，包括与高风险人工智能系统的预期使用对象相关的个人或群体。此外，数据集还应特别注意减少数据集中可能存在的偏差，这些偏差可能会影响个人的健康和安全，对基本权利产生负面影响，或导致欧盟法律禁止的歧视，尤其是在数据输出会影响未来操作的输入（“反馈回路”）的情况下。例如，偏差可能是基础数据集所固有的，特别是在使用历史数据时，或者是在现实世界环境中实施系统时产生的。人工智能系统提供的结果可能会受到这些固有偏差的影响，这些偏差可能会逐渐增加，从而延续和扩大现有的歧视，特别是对属于特定的弱势群体（包括种族或族裔群体）的人的歧视。在开发和测试人工智能系统时，要求数据集尽可能完整无误不应影响隐私保护技术的使用。特别是，数据集应在其预期目的要求的范围内，考虑到人工智能系统预期使用的特定地理、背景、行为或功能环境所特有的特征、特性或要素。与数据管理相关的要求可通过求助于提供认证合规服务的第三方来遵守，这些服务包括验证数据管理、数据集完整性以及数据培训、验证和测试实践，只要确保符合本条例的数据要求即可。

(45) 为了开发和评估高风险人工智能系统，特定的行为者，如提供者、通知机关和其他相关实体，如数字创新中心、测试实验设施和研究人员，应能够在各自活动领域内获取和使用与本条例相关的高质量数据集。欧盟委员会建立的欧洲共同数据空间，以及促进企业间和政府间在公共利益方面的数据共享，将有助于为人工智能系统的培训、验证和测试提供可信、负责和非歧视性的高质量数据访问。例如，在健康领域，欧洲健康数据空间将以保护隐私、安全、及时、透明和可信的方式，并通过适当的机构管理，促进对健康数据的非歧视性访问，并在这些数据集上对人工智能算法进行训练。提供或支持数据访问的相关主管机关，包括部门主管机关，也可支持为人工智能系统的培训、验证和测

试提供高质量数据。
(45a) 必须在人工智能系统的整个生命周期内保障隐私权和个人数据受保护的权利。在这方面，欧盟数据保护法规定的数据最小化原则和通过设计和默认方式保护数据的原则在处理个人数据时适用。提供者为确保遵守这些原则而采取的措施不仅包括匿名化和加密，还包括使用允许数据不动算法动的技术，以及允许在不影响本条例规定的数据管理要求的情况下，在各方之间传输或复制原始数据或结构化数据本身的情况下对人工智能系统进行训练。
44c 为了保护他人的权利免受人工智能系统中的偏见可能导致的歧视，在例外情况下，提供者应在确保对高风险人工智能系统进行偏见检测和纠正的严格必要范围内在对自然人的基本权利和自由采取适当保障措施的前提下，并在适用本条例规定的所有适用条件以及2016/679号条例、2016/680号指令和2018/1725号条例规定的条件之后，作为2016/679号条例第9条第2款第g项和2018/1725号条例第10条第2款第g项所指的重大公共利益事项，依然能够处理特殊类别的个人数据。
(46) 掌握关于高风险人工智能系统如何开发及其在整个生命周期中如何运行的可理解信息，对于实现这些系统的可追溯性、核实是否符合本条例的要求以及监测其运行情况和市场后监测至关重要。这就要求保存记录和提供技术文件，其中包含评估人工智能系统是否符合相关要求和促进市场后监测所需的信息。这些信息应包括系统的一般特点、能力和局限性，所使用的算法、数据、培训、测试和验证过程，以及相关风险管理系统的文件，并以清晰和全面的形式绘制。在人工智能系统的整个生命周期内，技术文件都应适当保持更新。此外，高风险人工智能系统应在技术上允许自动记录系统使用期间的事件，即日志。
(47) 为解决与特定的人工智能系统的不透明和复杂性有关的关切，并帮助部署者履行本条例规定的义务，应要求高风险人工智能系统在投放市场或投入使用前具备透明度。高风险人工智能系统的设计应使得部署者能够了解人工智能系统的工作原理，评估其功能，并理解其优势和局限性。高风险人工智能系统应附有适当的使用说明信息。这些信息应包括人工智能系统的特点、功能和性能限制。这些信息应包括与使用高风险人工智能系统有关的可能的已知和可预见情况，包括可能影响系统行为和性能的部署者行动，在这些情况下人工智能系统可能导致健康、安全和基本权利的风险，提供者预先确定和评估合格性的变化，以及相关的人工监督措施，包括便于部署者解释人工智能系统输出的措施。透明度，包括随附的使用说明，应有助于部署者使用系统并支持他们做出知情决策。除其他外，部署者应能更好地根据对其适用的义务正确选择他们意图使用的系统，了解预期的用途和排除的用途，并正确和适当地使用人工智能系统。为了提高使用说明中信息的可读性和易读性，在适当情况下，应包括举例说明，例如关于人工智能系统的局限性以及预期用途和排除用途。提供者应确保包括使用说明在内的所有文件都包含有意义、全面、可获取和可理解的信息，同时考虑到目标部署者的需求和可预见的知识。使用说明应以有关成员国确定的目标部署者易于理解的语言提供。
(48) 在设计和开发高风险人工智能系统时，应使自然人能够监督其运作，确保其按预期使用，并在系统的生命周期内消除其影响。为此，系统提供者应在系统投放市场或投入使用前确定适当的人工监督措施。特别是，在适当的情况下，这些措施应保证系统受到内置的操作限制，这些限制不能被系统本身所推

翻，并能对人类操作者做出反应，而且被指派进行人为监督的自然人应具有履行这一职责所必需的能力、培训和授权。此外，还必须酌情确保高风险人工智能系统包括一些机制，以指导和通知接受人工监督的自然人，使其在知情的情况下决定是否、何时以及如何进行干预，以避免负面后果或风险，或在系统未按预期运行时停止运行。考虑到某些生物鉴别系统的错误匹配会对个人造成严重后果，因此，宜规定对这些系统加强人的监督，以便部署者不得根据该系统产生的识别结果采取任何行动或做出任何决定，除非至少有两个自然人分别加以核实和确认。这些人可以来自一个或多个实体，包括操作或使用系统的人。这项要求不应造成不必要的负担或延误，只要将不同人员的单独核实自动记录在系统生成的日志中即可。鉴于执法、移民、边境管制和庇护等领域的特殊性，在欧盟或国家法律认为适用这一要求不成比例的情况下，不应适用这一要求。

(49) 高风险人工智能系统应在其整个生命周期内始终如一地运行，并根据其预期目的和公认的技术水平，达到适当的准确性、稳健性和网络安全水平。鼓励委员会和相关组织及利益相关方适当考虑降低人工智能系统的风险和负面影响。应在随附的使用说明中宣布预期的性能指标水平。敦促提供者以清晰易懂的方式向部署者传达这一信息，避免误解或误导性陈述。

欧盟关于法定计量的立法，包括《计量仪器指令》（MID）和《非自动称重仪器指令》（NAWI），旨在确保计量准确性，并帮助提高商业交易的透明度和公平性。在此背景下，委员会应与利益相关的各方和组织，如计量和基准制定机构合作，酌情鼓励制定人工智能系统的基准和测量方法。在此过程中，委员会应注意到从事与人工智能有关的计量学和相关衡量指标工作的国际合作伙伴，并与其开展合作。

(50) 技术稳健性是高风险人工智能系统的关键要求。这些系统应能抵御因系统内部限制或系统运行环境，如错误、故障、不一致、意外情况而导致的有害或其他不良行为。因此，应采取技术和组织措施，确保高风险人工智能系统的稳健性，例如设计和开发适当的技术解决方案，以防止或尽量减少有害或不良行为。例如，这些技术解决方案可包括使系统在出现某些异常情况或运行超出某些预定边界时安全中断其运行的机制，即故障安全计划。如果不能防范这些风险，可能会导致安全影响或对基本权利产生负面影响，例如，由于人工智能系统产生的错误决定或错误或有偏见的输出。

(51) 网络安全在确保人工智能系统具有抵御恶意第三方利用系统漏洞改变其使用、行为、性能或破坏其安全属性的能力方面发挥着至关重要的作用。针对人工智能系统的网络攻击可以利用人工智能的特定资产，如针对训练数据集的数据投毒或针对训练模型的对抗性攻击或成员推理，或利用人工智能系统数字资产或底层信息和通信技术基础设施中的漏洞。因此，为确保网络安全水平与风险相适应，高风险人工智能系统的提供者应采取适当措施，如安全控制，并酌情考虑底层信息和通信技术基础设施。

(51a) 在不影响本条例规定的稳健性和准确性要求的前提下，根据2022/0272号条例第8条，属于2022/0272号条例范围内的高风险人工智能系统可通过满足2022/0272号条例第10条和附件规定的基本网络安全要求来证明符合本条例的网络安全要求。当高风险人工智能系统满足2022/0272号条例的基本要求时，只要根据2022/0272号条例发布的欧盟合格性声明或部分合格性声明证明达到了这些要求，就应视为符合本条例规定的网络安全要求。为此，根据2022/0272号法

规，对根据本法规被归类为高风险人工智能系统的具有数字元素的产品进行网络安全风险评估时，应考虑人工智能系统在未经授权的第三方试图改变其使用、行为或性能方面的网络韧性风险，包括人工智能特有的漏洞，如数据投毒或对抗性攻击，以及本法规要求的相关基本权利风险。
本条例规定的合格性评估程序应适用于具备由2022/0272号条例所涵盖的数字元素并根据本条例被归类为高风险人工智能系统的产品的基本网络安全要求。然而，该规则不应导致降低2022/0272号法规所涵盖的具有数字元素的关键产品的必要保证水平。因此，作为本规则的克减，属于本条例范围内的高风险人工智能系统，同时根据第2022/0272号条例被定性为具有数字元素的重要和关键产品，并且本条例附件六中提及的基于内部控制的合格性评估程序适用于该系统，就2022/0272号条例的基本网络安全要求而言，该系统须遵守2022/0272号条例的合格性评估规定。在这种情况下，对于本条例涵盖的所有其他方面，应适用本条例附件六中基于内部控制的合格性评估规定。基于ENISA在网络安全政策方面的知识和专长，以及根据2019/1020号条例分配给ENISA的任务，委员会应与 ENISA 就人工智能系统的网络安全相关问题开展合作。
(52) 作为欧盟统一立法的一部分，适用于高风险人工智能系统投放市场、投入使用和使用的规则应与欧洲议会和理事会765/2008号条例[22]一致，该条例规定了产品认证和市场监督的要求、欧洲议会和欧盟理事会关于产品营销共同框架的768/2008/EC号决定[23]以及欧洲议会和欧盟理事会关于产品市场监督和合规性2019/1020号条例[24]（《产品营销的新立法框架》）。
(53) 由一个特定的自然人或法人，定义为提供者负责将高风险人工智能系统投放市场或投入使用是适当的，无论该自然人或法人是否是设计或开发该系统的人。
(53a) 作为《联合国残疾人权利公约》(UNCRPD)的签署国，欧盟和成员国在法律上有义务保护残疾人不受歧视，促进其平等对待，确保残疾人在与其他人平等的基础上获得信息和通信技术和系统，并确保尊重残疾人的隐私。鉴于人工智能系统的重要性和使用量日益增加，在所有新技术和服务中应用通用设计原则，应确保每个可能受人工智能技术影响或使用人工智能技术的人，包括残疾人，都能以充分考虑其固有尊严和多样性的方式，充分和平等地使用人工智能技术。因此，提供者必须确保完全符合无障碍要求，包括2016/2102号指令和2019/882号指令。提供者应确保在设计上符合这些要求。因此，应尽可能将必要措施纳入高风险人工智能系统的设计中。
(54) 提供者应建立健全的质量管理体系，确保完成规定的合格性评估程序，起草相关文件，并建立健全的后市场监测体系。高风险人工智能系统的提供者，如果根据相关的欧盟部门法有义务建立质量管理体系，则应有可能将本条例规定的质量管理体系要素作为其他欧盟部门法规定的现有质量管理体系的一部分。在未来的标准化活动或欧盟委员会通过的指南中，也应考虑本条例与现行欧盟部门法之间的互补性。公共机关为其自身使用的高风险人工智能系统提供

[22] 欧洲议会和理事会 2008 年 7 月 9 日 765/2008 号条例规定了与产品销售有关的认证和市场监督要求，并废除 339/93 号条例（官方公报，L 218，2008 年 8 月 13 日，第 30 页）。
[23] 欧洲议会和理事会 2008 年 7 月 9 日关于产品营销共同框架的 768/2008/EC 号决定，废除理事会 93/465/EEC 号决定（官方公报，L 218，2008 年 8 月 13 日，第 82 页）。
[24] 欧洲议会和欧盟理事会 2019 年 6 月 20 日关于市场监督和产品合规性的 2019/1020 号条例，修订 2004/42/EC 号指令以及 765/2008 号和 305/2011 号条例（与欧洲经济区相关的文本）（官方公报，L 169，2019 年 6 月 25 日，第 1-44 页）。

服务时，可酌情采用和实施质量管理体系规则，作为在国家或地区一级采用的质量管理体系的一部分，同时考虑到该部门的特殊性以及相关公共机关的权限和组织。

(56) 为了能够执行本条例并为经营者创造一个公平竞争的环境，同时考虑到提供数字产品的不同形式，必须确保在任何情况下，在欧盟设立的个人都能向机关提供关于人工智能系统合规性的所有必要信息。因此，在欧盟境外设立的提供者在欧盟境内提供其人工智能系统之前，应通过书面授权任命一名在欧盟境内设立的授权代表。该授权代表发挥关键作用，确保未在欧盟设立机构的提供者在欧盟投放市场或投入使用的高风险人工智能系统合规，并担任其在欧盟设立的联系人。

(56a) 鉴于人工智能系统价值链的性质和复杂性，并且根据《新立法框架》的原则，必须确保法律的确定性并促进对本条例的遵守。因此，有必要明确价值链上相关经营者的作用和具体义务，如可能促进人工智能系统发展的进口者和分销者。在特定情况下，这些经营者可能会同时扮演多个角色，因此应累计地履行与这些角色相关的所有义务。例如，经营者可同时担任分销者和进口者。

(57) 为了确保法律的确定性，有必要澄清，在特定的条件下，任何分销者、进口者、部署者或其他第三方都应视为高风险人工智能系统的提供者，并因此承担所有相关义务。如果该方在已投放市场或投入使用的高风险人工智能系统上冠以自己的名称或商标，尽管如此行事不妨碍合同中规定以其他方式分配义务的安排，或者如果该方对已投放市场或投入使用的高风险人工智能系统进行实质性修改，使其仍然属于第6条所指的高风险人工智能系统，则属于这种情况，或者如果其修改了一个人工智能系统，包括通用人工智能系统的预期用途，而该人工智能系统尚未被归类为高风险系统，并且已经投放市场或投入使用，根据第6条的规定，该人工智能系统成为高风险人工智能系统。这些规定的适用不应妨碍本条例应与之共同适用的特定的新立法框架部门立法中的具体规定。例如，745/2017号条例第16条第2款规定，特定的修改不应视为可能影响其符合适用要求的设备修改，应继续适用于属于该法规意义上的医疗设备的高风险人工智能系统。

(57a) 通用人工智能系统本身可用作高风险人工智能系统，也可作为其他高风险人工智能系统的组成部分。因此，由于其特殊性，并为了确保在人工智能价值链上公平分担责任，除非本条例另有规定，否则此类系统的提供者应与相关高风险人工智能系统的提供者密切合作，使其能够遵守本条例规定的相关义务，并遵守根据本条例设立的主管机关的规定。

(57b) 如果根据本条例规定的条件，最初将人工智能系统投放市场或投入使用的提供者不应再视为本条例意义上的提供者，而且该提供者没有明确排除将人工智能系统转变为高风险人工智能系统的可能性，则先前的提供者仍应密切合作，提供必要的信息，并提供合理预期的技术准入和其他协助，以履行本条例规定的义务，特别是关于高风险人工智能系统合格性评估的义务。

(57c) 此外，如果高风险人工智能系统是相关新立法框架部门立法所涵盖的产品的一个安全组件，而该系统没有独立于产品投放市场或投入使用，则相关新立法框架立法所定义的产品制造商应遵守本条例所规定的提供者的义务，并特别确保嵌入最终产品中的人工智能系统符合本条例的要求。

(57d) 在人工智能价值链中，多个相关方往往不仅提供人工智能系统、工具和服务， 而且还提供由提供者纳入人工智能系统的组件或流程，其目的有多种，

包括模型训练、模型再训练、模型测试和评估、纳入软件或模型开发的其他方面。这些当事方在面向高风险人工智能系统提供者的价值链中发挥着重要作用，其人工智能系统、工具、服务、组件或流程被集成到该系统中，并应通过书面协议向该提供者提供必要的信息、能力、技术访问和基于先进技术水平的其他援助，以使提供者能够在不损害其自身知识产权或商业秘密的情况下完全遵守本条例规定的义务。

(57e) 向公众提供工具、服务、流程或人工智能组件，通用人工智能模型除外，的第三方，如果这些工具、服务、流程或人工智能组件是在免费和开源许可下提供的，则不应强制要求其遵守针对人工智能价值链责任的要求，特别是针对使用或集成这些工具、服务、流程或人工智能组件的提供者的要求。除通用人工智能模型外，应鼓励免费开源工具、服务、流程或人工智能组件的开发者实施广泛采用的文档实践，如模型卡和数据卡，以此加快人工智能价值链上的信息共享，从而在欧盟推广值得信赖的人工智能系统。

(57f) 委员会可制定并建议高风险人工智能系统提供者与提供高风险人工智能系统所使用或集成的工具、服务、组件或流程的第三方之间的自愿示范合同条款，以促进价值链上的合作。在制定自愿示范合同条款时，委员会还应考虑到适用于特定部门或商业案例的可能合同要求。

(58) 鉴于人工智能系统的性质及其使用可能对安全和基本权利造成的风险，包括需要确保适当监测人工智能系统在现实生活中的表现，为部署者规定具体的责任是适当的。部署者尤其应采取适当的技术和组织措施，确保其按照使用说明使用高风险的人工智能系统，并应酌情规定监测人工智能系统运作和保存记录方面的某些其他义务。此外，部署者应确保被指派执行本条例规定的使用说明和人工监督的人员具备必要的能力，特别是适当的人工智能知识水平、培训和适当履行这些任务的权力。这些义务不应影响欧盟或国家法律规定的与高风险人工智能系统有关的其他部署者义务。

(58b) 本条例不妨碍雇主根据欧盟或国家法律和惯例，包括关于向雇员通报和咨询的一般框架的2002/14/EC号指令，就投入使用人工智能系统的决定向工人或其代表通报或通报和咨询的义务。在其他法律文书中规定的信息或信息和咨询义务未得到满足的情况下，仍有必要确保工人及其代表了解在工作场所部署高风险人工智能系统的计划。此外，这种知情权对于本条例所依据的保护基本权利的目标是辅助和必要的。因此，本条例应规定这方面的信息要求，而不影响工人的任何现有权利。

(58b) 虽然与人工智能系统有关的风险可能来自此类系统的设计方式，但风险也可能来自此类人工智能系统的使用方式。因此，高风险人工智能系统的部署者在确保基本权利得到保护方面起着至关重要的作用，是对提供者在开发人工智能系统时所承担义务的补充。部署者最了解高风险人工智能系统将如何具体使用，因此能够识别开发阶段未预见的潜在重大风险，因为部署者更准确地了解使用环境、可能受影响的人群或群体，包括弱势群体。附件三提到的高风险人工智能系统的部署者在向自然人提供信息方面也起着关键作用，在做出或协助做出与自然人有关的决定时，部署者应酌情向自然人提供信息，告知其将使用高风险人工智能系统。这些信息应包括预期目的和决策类型。部署者还应告知自然人其有权获得本条例规定的解释。对于用于执法目的的高风险人工智能系统，应根据2016/680号指令第13条履行这一义务。

(58d) 为执法目的使用人工智能系统进行生物特征识别时涉及的任何生物特征

数据处理都需要遵守2016/680号指令第10条，该条规定，只有在严格必要的情况下，在适当保障数据主体的权利和自由的前提下，并经欧盟或成员国法律授权，才允许进行此类处理。在获得授权的情况下，此类使用还需遵守2016/680号指令第4条第1款规定的原则，包括合法性、公平性和透明度、目的限制、准确性和存储限制。

(58e) 在不影响适用的欧盟法律，特别是《通用数据保护条例》和2016/680号指令的情况下，考虑到远程事后生物特征识别系统的侵入性，远程事后生物特征识别系统的使用应受到保障措施的约束。事后生物识别系统的使用应始终做到适度、合法且严格必要，因此在识别的个人、地点、时间范围方面应具有针对性，并以合法获取的视频录像的封闭数据集为基础。在任何情况下，事后远程生物识别系统都不应用于执法框架，导致普遍性的监视。在任何情况下，事后远程生物识别的条件都不应成为规避实时远程生物识别的禁止条件和严格例外的依据。

(58g) 为了有效确保基本权利得到保护，受公法管辖的高风险人工智能系统的部署者，或提供公共服务的私人运营商和部署附件三所述的特定高风险人工智能系统的运营商，如银行或保险实体，应在投入使用前进行基本权利影响评估。私人实体也可以提供对个人重要的公共服务。提供此类公共性服务的私人运营商与公共利益任务相关，如教育、医疗保健、社会服务、住房、司法管理等领域。基本权利影响评估的目的是让部署者确定可能受影响的个人或个人群体的权利所面临的具体风险，并确定在这些风险具体化的情况下应采取的措施。影响评估应确定部署者按照预期目的使用高风险人工智能系统的相关程序，并应包括对意图使用该系统的时间段和频率以及在具体使用环境中可能受到影响的自然人和群体的具体类别的描述。评估还应包括确定可能影响这些人或群体基本权利的具体伤害风险。在进行评估时，部署者应考虑到与适当评估影响有关的信息，包括但不限于高风险人工智能系统提供者在使用说明中提供的信息。根据所确定的风险，部署者应确定在这些风险成为现实的情况下应采取的措施，例如包括在具体使用情况下的治理安排，如根据使用说明进行人为监督的安排，或投诉处理和补救程序，因为这些安排在具体使用情况下可能有助于减轻对基本权利的风险。在进行影响评估后，部署者应通知相关市场监督管理机关。在适当情况下，为收集进行影响评估所需的相关信息，高风险人工智能系 统的部署者，特别是在公共部门使用人工智能系统时，可让利益相关方，包括可能受人工智能系统影响的群体的代表、独立专家和公民社会组织参与进行这种影响评估，并设计在风险具体化的情况下应采取的措施。人工智能办公室应开发一个调查问卷模板，以促进遵守和减少部署者的行政负担。

(60a) 应明确界定通用人工智能模型的概念，并将其与人工智能系统的概念区分开来，以确保法律的确定性。定义应基于通用人工智能模型的关键功能特征，特别是通用性和胜任各种不同任务的能力。这些模型通常通过自我监督、无监督或强化学习等各种方法在大量数据上进行训练。通用人工智能模型可以通过各种方式投放市场，包括通过库、应用编程接口（API）、直接下载或实物拷贝。这些模型可以进一步修改或微调为新的模型。虽然人工智能模型是人工智能系统的重要组成部分，但其本身并不构成人工智能系统。人工智能模型需要添加更多的组件，例如用户界面，才能成为人工智能系统。人工智能模型通常被集成到人工智能系统中，成为人工智能系统的一部分。本条例为通用人工智能模型和构成系统风险的通用人工智能模型提供了具体规则，这些规则也应

适用于这些模型被集成到人工智能系统中或构成人工智能系统的一部分的情况。应该理解的是，一旦通用人工智能模型投放市场，通用人工智能模型提供者的义务就应适用。当通用人工智能模型的提供者将自己的模型集成到自己的人工智能系统中并在市场上销售或投入使用时，该模型应被视为已投放市场，因此，除人工智能系统的义务外，本条例中有关模型的义务也应继续适用。在任何情况下，当自有模型用于纯粹的内部流程，而这些流程对于向第三方提供产品或服务并不重要，且自然人的权利不受影响时，本条例中针对模型规定的义务不应适用。考虑到其潜在的重大负面影响，具有系统性风险的通用人工智能模型应始终遵守本条例规定的相关义务。该定义不应涵盖在投放市场前仅用于研究、开发和原型设计活动的人工智能模型。这并不影响在此类活动之后将模型投放市场时遵守本条例的义务。

(60b) 虽然模型的通用性也可以通过参数数量等标准来确定，但至少有十亿个参数并使用大量数据通过大规模自监督进行训练的模型，应视为显示出显著的通用性，并且能够胜任各种不同的任务。

(60c) 大型生成式人工智能模型是通用人工智能模型的典型范例，因为它们可以灵活地生成内容，如文本、音频、图像或视频形式的内容，可随时适应各种不同的任务。

(60d) 当一个通用人工智能模型集成到一个人工智能系统中或成为其组件之一时，该系统应视为一个通用人工智能系统，因为这种集成使该系统有能力服务于各种目的。通用人工智能系统可以直接使用，也可以集成到其他人工智能系统中。

(60e) 通用人工智能模型的提供者在人工智能价值链中具有特殊的作用和责任，因其所提供的模型可能构成一系列下游系统的基础，而这些系统往往是由下游提供者提供的，下游提供者需要充分了解模型及其功能，以便能够将这些模型集成到他们的产品中，并履行本条例或其他条例规定的义务。因此，应预见适度的透明度措施，包括起草和不断更新文件，以及提供有关通用人工智能模型的信息，供下游提供者使用。技术文件应由通用人工智能模型提供者编制并不断更新，以便在人工智能办公室和国家主管机关提出要求时提供给它们。附件XY和附件XX应分别概述此类文件中包含的最基本的要件。委员会应能够根据不断发展的技术，通过授权法案对附件进行修订。

(60i) 包括模型在内的软件和数据在免费且开源许可下发布，允许公开共享，用户可以自由访问、使用、修改和重新发布这些软件和数据或其修改版本，可以促进市场研究和创新，并为联盟经济提供重要的增长机会。在免费且开源许可下发布的通用人工智能模型，如果其参数，包括权重、模型架构信息和模型使用信息是公开的，则应视为确保了高水平的透明度和开放性。如果许可允许用户运行、复制、分发、研究、更改和改进软件和数据，包括模型，但必须注明模型的原始提供者，并遵守相同或类似的分发条款，那么相应许可也应被视为免费且开源的。

(60i+1) 免费且开源的人工智能组件涵盖了软件和数据，包括模型和通用人工智能模型、工具、服务或人工智能系统的流程。免费和开源人工智能组件可通过不同的渠道提供，包括在开放存储库中开发。就本条例而言，有偿提供或以其他方式商业化的人工智能组件，包括通过软件平台提供与人工智能组件相关的技术支持或其他服务，或出于改善软件安全性、兼容性或互操作性以外的原因使用个人数据，不应享受免费和开源人工智能组件的例外规定，但微型企业

之间的交易除外。通过开源提供人工智能组件这一事实本身不应构成商业化。
(60f) 通用人工智能模型的提供者，如果其模型参数，包括权重、模型结构信息和模型使用信息，是在免费且开源的许可下发布的，则应在通用人工智能模型的透明度相关要求方面享有例外，除非这些模型被认为会带来系统性风险，在这种情况下，模型是透明的并附有开源许可，不应被视为排除遵守本条例规定的义务的充分理由。
在任何情况下，鉴于在免费且开源许可下发布通用人工智能模型并不一定披露有关用于模型训练或微调的数据集以及如何确保尊重版权法的大量信息，因此为通用人工智能模型提供的不遵守透明度相关要求的例外情况不应涉及编制有关模型训练所用内容的摘要的义务，以及制定尊重欧盟版权法的政策的义务，特别是确定和尊重根据2019/790号指令第4条第3款表达的权利保留的义务。
(60g) 对通用人工智能模型提供者所规定义务的遵守，应与模型提供者的类型相适应且成比例，排除为非专业或科学研究目的开发或使用模型者遵守义务的需要，但应鼓励其自愿遵守这些要求。在不影响欧盟版权法的情况下，遵守这些义务应适当考虑提供者的规模，并允许小微型企业，包括初创企业，以简化的方式遵守这些义务，但不应造成过高的成本，也不应阻碍对这些模型的使用。在对模型进行修改或微调的情况下，提供者的义务应仅限于修改或微调，例如，在现有的技术文件中补充有关修改的信息，包括新的训练数据源，以此来遵守本条例规定的价值链义务。
(60i) 通用模型，特别是能够生成文本、图像和其他内容的大型生成模型，为艺术家、作家和其他创作者及其创作内容的创作、传播、使用和消费方式带来了独特的创新机遇，但也带来了挑战。开发和训练此类模型需要获取大量文本、图像、视频和其他数据。在这种情况下，文本和数据挖掘技术可广泛用于检索和分析这些内容，而这些内容可能受到版权和相关权利的保护。对受版权保护内容的任何使用都必须获得相关权利人的授权，除非适用相关的版权例外和限制。2019/790号指令引入了例外和限制，允许在特定条件下为文本和数据挖掘的目的复制和提取作品或其他主体。根据这些规则，权利人可以选择保留对其作品或其他主体的权利，以防止文本和数据挖掘，除非是为了科学研究的目的。在以适当方式明确保留选择退出权的情况下，通用人工智能模型的提供者如果想对这些作品进行文本和数据挖掘，需要获得权利人的授权。
(60j) 将通用人工智能模型投放到欧盟市场的提供者应确保遵守本条例中的相关义务。为此，通用人工智能模型提供者应制定政策，尊重欧盟关于版权和相关权利的法律，特别是识别和尊重权利人根据2019/790号指令第4条第3款表达的权利保留。任何将通用人工智能模型投放到欧盟市场的提供者都应遵守这一义务，无论这些通用人工智能模型的培训所依据的版权相关行为发生在哪个司法管辖区。这对于确保通用人工智能模型提供者之间的公平竞争环境是必要的，任何提供者都不能通过采用低于欧盟规定的版权标准在欧盟市场上获得竞争优势。
(60k) 为了提高通用人工智能模型的预训练和训练中使用的数据的透明度，包括受版权法保护的文本和数据，此类模型的提供者应就通用模型训练中使用的内容制定并公开足够详细的摘要。在适当考虑保护商业秘密和商业机密信息的同时，该摘要的范围应总体上全面而不是技术上详细，以方便包括版权持有者在内的合法权益方行使和执行其在欧盟法律下的权利，例如列出用于训练模型的主要数据收集或数据集，如大型私人或公共数据库或数据档案，并对所使用

的其他数据来源进行叙述性的解释。人工智能办公室宜提供一个摘要模板，该模板应简单、有效，并允许提供者以叙述形式提供所需的摘要。
(60ka) 关于对通用人工智能模型提供者规定的义务，即制定尊重欧盟版权法的政策，并公开提供用于培训的内容摘要，人工智能办公室应监督提供者是否履行了这些义务，而不对培训数据的版权合规性进行逐项核查或评估。本条例不影响欧盟法律规定的版权规则的执行。
(60m) 通用人工智能模型可能带来系统性的风险，其中包括但不限于：与重大事故、关键部门中断和对公众健康与安全的严重后果有关的任何实际的或可合理预见的负面影响；对民主进程、公共和经济安全的任何实际的或可合理预见的负面影响；非法、虚假或歧视性内容的传播。系统性风险应被理解为随着模型能力和模型范围的增加而增加，可能在模型的整个生命周期中出现，并受到滥用条件、模型可靠性、模型公平性和模型安全性、模型自主程度、获取工具的途径、新颖或组合模式、发布和传播策略、移除护栏的可能性和其他因素的影响。特别是，迄今为止，国际层面的进路已确定需要关注以下风险：潜在的故意滥用或与人类意图对齐的并非故意的控制问题；化学、生物、辐射和核风险，如降低准入门槛的方式，包括武器开发、设计获取或使用；攻击性网络能力，如发现、利用或操作使用漏洞的方式；交互作用和工具使用的影响，包括控制物理系统和干扰关键基础设施的能力等；模型复制自身或“自我复制”或训练其他模型的风险；模型可能导致有害偏见和歧视的方式，给个人、社区或社会带来风险；为虚假信息提供便利或损害隐私，给民主价值观和人权带来威胁；特定事件可能导致连锁反应，产生相当大的负面影响，可能影响到整个城市、整个领域的活动或整个社区。
(60n) 建立一种将通用人工智能模型分类为具有系统风险的通用人工智能模型的方法是适当的。由于系统性风险源于特别高的能力，如果通用人工智能模型根据适当的技术工具和方法进行评估，具有高影响能力，或由于其影响范围而对内部市场产生重大影响，则应将其视为具有系统性风险。通用人工智能模型中的高影响能力是指与最先进的通用人工智能模型中记录的能力相匹配或超过这些能力的能力。在模型投放市场后或用户与模型互动时，可以更好地了解模型的全部能力。根据本条例生效时的技术水平，以浮点运算数（FLOPs）衡量的通用人工智能模型训练所用的累计计算量是模型能力的相关近似值之一。用于训练的计算量是在部署前旨在提高模型能力的各项活动和方法（如预训练、合成数据生成和微调）中所用计算量的累积。因此，应设定一个FLOPs的初始阈值，如果通用人工智能模型达到了这个阈值，就可以推定该模型是一个具有系统风险的通用人工智能模型。这一阈值应随着时间的推移而调整，以反映技术和产业的变化，如算法的改进或硬件效率的提高，并应辅以模型能力的基准和指标。为此，人工智能办公室应与科学界、产业界、公民社会和其他专家合作。用于评估高影响力能力的阈值以及工具和基准，应当能够有力地预测通用人工智能模型的通用性、能力和相关系统风险，并可考虑到模型投放市场的方式或可能影响的用户数量。作为对这一制度的补充，如果发现某个通用人工智能模型的能力或影响等同于设定阈值所涵盖的能力或影响，则委员会应有可能做出个别决定，将该模型指定为具有系统性风险的通用人工智能模型。这一决定应基于对附件YY所列标准的整体评估，如训练数据集的质量或规模、业务和最终用户的数量、其输入和输出模态、其自主程度和可扩展性，或其可使用的工具。如果模型被指定为具有系统性风险的通用人工智能模型的提供者提出合

理的请求，委员会应考虑该请求，并可决定重新评估该通用人工智能模型是否仍可被视为具有系统性风险。
(60o) 还有必要明确具有系统风险的通用人工智能模型的分类的程序。达到高影响能力适用阈值的通用人工智能模型应被推定为具有系统风险的通用人工智能模型。提供者最迟应在满足要求或得知通用人工智能模型将满足导致推定的要求两周后通知人工智能办公室。这一点与FLOPs门槛尤其相关，因为通用人工智能模型的培训需要大量的规划，包括计算资源的前期分配，因此，通用人工智能模型的提供者能够在培训完成之前就知道其模型是否会达到阈值。在此通知的背景下，提供者应当能够证明，由于其特殊性，通用人工智能模型在特殊情况下不会带来系统性风险，因此不应被归类为具有系统性风险的通用人工智能模型。这些信息对于人工智能办公室预测具有系统风险的通用人工智能模型的市场投放很有价值，提供者可以尽早开始与人工智能办公室接触。这对于计划以开源方式发布的通用人工智能模型尤为重要，因为在开源模型发布后，确保遵守本条例规定义务的必要措施可能更难实施。
(60p) 如果委员会意识到一个通用人工智能模型符合归类为具有系统性风险的通用模型的要求，而以前并不知道或相关提供者没有通知委员会，委员会应有权将其归类为具有系统性风险的通用模型。除了人工智能办公室的监测活动外，有条件的警报系统应确保人工智能办公室从科学小组那里了解到有可能被归类为具有系统风险的通用人工智能模型。
60q) 对于存在系统性风险的通用人工智能模型的提供者，除了为通用人工智能模型的提供者规定的义务外，还应规定旨在识别和减轻这些风险并确保适当水平的网络安全保护的义务，无论是作为独立模型提供还是嵌入人工智能系统或产品中提供。为实现这些目标，该条例应要求提供者对模型进行必要的评估，特别是在首次投放市场之前，包括对模型进行对抗测试并记录在案，也可酌情通过内部或独立外部测试进行。此外，具有系统性风险的通用人工智能模型的提供者应持续评估和降低系统性风险，包括例如制定风险管理政策，如问责制和治理流程，实施后市场监测，在整个模型生命周期内采取适当措施，并与整个人工智能价值链的相关参与者合作。
(60r) 具有系统风险的通用人工智能模型的提供者应评估和减轻可能的系统风险。如果尽管努力识别和预防与可能带来系统性风险的通用人工智能模型有关的风险，但该模型的开发或使用造成了严重事故，通用人工智能模型提供者应毫不拖延地跟踪该事故，并向委员会和国家主管机关报告任何相关信息和可能的纠正措施。此外，在整个模型生命周期内，提供者应酌情确保对模型及其物理基础设施提供适当水平的网络安全保护。与恶意使用或攻击相关的系统性风险的网络安全保护应充分考虑模型的意外泄漏、未经许可的发布、规避安全措施，以及防御网络攻击、未经授权的访问或模型失窃。可以通过确保模型权重、算法、服务器和数据集的安全来促进这种保护，例如通过信息安全的操作安全措施、具体的网络安全政策、适当的技术和既定解决方案，以及网络和物理访问控制，以适应相关情况和所涉及的风险。
(60s) 人工智能办公室应鼓励和促进行为守则的起草、审查和修改，同时考虑到国际的进路。可以邀请所有通用人工智能模型的提供者参与。为确保行为守则反映最新情况并适当考虑到各种不同的观点，人工智能办公室应与相关国家主管机关合作，并可酌情与公民社会组织和其他利益相关方和专家，包括科学小组协商，以起草守则。行为守则应涵盖通用人工智能模型和具有系统风险的

通用模型提供者的义务。此外，关于系统性风险，行为守则应有助于在联盟层面建立系统性风险类型和性质的风险分类，包括其来源。行为守则还应侧重于具体的风险评估和缓解措施。

(60t) 行为守则应当成为通用人工智能模型提供者正确履行本条例规定义务的核心工具。提供者应能依靠行为守则来证明其遵守了相关义务。通过实施法案，委员会可决定批准一项行为守则，并使其在联盟内具有普遍效力，或者，如果在本条例开始适用时，行为守则无法最终确定，或人工智能办公室认为其不够充分，委员会也可决定为履行相关义务提供共同规则。一旦统一标准公布并被人工智能办公室评估为适合于涵盖相关义务，遵守统一标准的提供者应被推定为具备合格性。此外，如果没有行为守则或统一标准，或选择不依赖这些规范或标准，通用人工智能模型的提供者应能够使用其他适当的方法来证明其合格性。

(60u) 本条例对人工智能系统和模型进行监管，对将其投放市场、投入使用或在欧盟使用的相关市场行为者规定了某些要求和义务，从而补充了2022/2065号条例对将此类系统或模型嵌入其服务的中介服务提供者规定的义务。如果这些系统或模型被嵌入到指定的超大型在线平台或超大型在线搜索引擎中，则须遵守2022/2065号法规规定的风险管理框架。《人工智能法》的相应义务因而应应推定为已经履行，除非在此类模型中出现并识别到了2022/2065号条例未曾涵盖的重大系统性风险。在此框架内，超大型在线平台和超大型搜索引擎的提供者有义务评估其服务的设计、运作和使用所产生的潜在系统性风险，包括服务中使用的算法系统的设计如何可能导致此类风险，以及潜在滥用所产生的系统性风险。这些提供者还有义务采取适当的缓解措施，以尊重基本权利。

(60aa)考虑到不同的欧盟法律文件的适用范围内数字服务的快速创新和技术演进，特别是考虑到其接收者的使用和感知，本条例所涉及的人工智能系统可作为2022/2065号条例意义上的中介服务或部分中介服务提供，该条例应以技术中立的方式进行解释。例如，人工智能系统可用于提供在线搜索引擎，特别是在人工智能系统，如在线聊天机器人，原则上对所有网站进行搜索，然后将搜索结果纳入其现有知识，并使用更新后的知识生成结合不同信息来源的单一输出的情况下。

(60v) 此外，本条例规定特定的人工智能系统的提供者和部署者有义务能够检测和披露这些系统的输出是人为生成或操纵的，这与促进有效实施2022/2065号条例特别相关。这尤其适用于超大型在线平台或超大型在线搜索引擎提供者的义务，即识别和降低因传播人为生成或操纵的内容而可能产生的系统性风险，特别是对民主进程、公民言论和选举进程产生实际或可预见负面影响的风险，包括通过虚假信息产生的风险。

(61) 标准化应发挥关键作用，为提供者提供技术解决方案，确保其符合本法规，并与最新技术保持一致，以促进创新以及单一市场的竞争力和增长。遵守欧洲议会和欧盟理事会1025/2012号条例[25]中定义的统一标准应成为提供者证明符合本法规要求的一种手段，这些标准通常应反映先进技术水平。因此，应根据1025/2012号法规第5条和第6条，鼓励所有利益相关方，特别是小微型企业、

[25] 欧洲议会和欧盟理事会 2012 年 10 月 25 日关于欧洲标准化的 1025/2012 号条例，修订欧洲议会和欧盟理事会 89/686/EEC 号和 93/15/EEC 号指令以及 94/9/EC 号、94/25/EC 号、95/16/EC 号、97/23/EC 号、98/34/EC 号、2004/22/EC 号、2007/23/EC 号、2009/23/EC 号和 2009/105/EC 号指令，并废除欧洲议会和欧盟理事会 87/95/EEC 号决定和 1673/2006/EC 号决定（官方公报，L 316，14.11.2012，第 12 页）。

消费者组织以及环境和社会利益相关方参与标准制定，以实现利益平衡。为了促进合规，委员会应及时发布标准化申请。在准备标准化要求时，委员会应咨询人工智能咨询论坛和理事会，以收集相关专业知识。
然而，在没有相关统一标准可供参考的情况下，欧盟委员会应能够通过实施法案，并在与人工智能咨询论坛协商后，为本条例下的特定要求制定共同规格。当标准化要求未被任何欧洲标准化组织接受时，或当相关统一标准未能充分解决基本权利问题时，或当统一标准不符合要求时，或当适当的统一标准迟迟未被采用时，共同规则应作为一种特殊的备用解决方案，以促进提供者履行遵守本条例要求的义务。如果由于有关标准的技术复杂性而导致统一标准迟迟未获通过，委员会在考虑制定共同规格之前应考虑到这一点。在制定共同规则时，鼓励委员会与国际合作伙伴和国际标准化机构合作。
(61a) 在不影响使用统一标准和共同规格的情况下，高风险人工智能系统的提供者，如果其经过训练和测试的数据反映了人工智能系统意图使用的特定的地理、行为、场景或功能环境，则应推定为符合本条例规定的数据管理要求中的相关措施。
在不影响本条例规定的稳健性和准确性相关要求的情况下，根据欧洲议会和理事会2019/881号条例第54条第3款、只要网络安全认证或合格性声明或其部分内容涵盖了本条例的网络安全要求，则应推定已根据该条例的网络安全计划获得认证或已发布合格性声明的高风险人工智能系统符合本条例的网络安全要求，且其参考文件已在《欧盟官方公报》上公布。
(62) 为了确保高风险人工智能系统的高度可信性，这些系统在投放市场或投入使用之前应接受合格性评估。
(63) 为了最大限度地减轻操作者的负担并避免任何可能的重复，对于采用新立法框架方法的现有欧盟统一立法所涵盖的与产品有关的高风险人工智能系统，应将这些人工智能系统是否符合本条例的要求作为该立法已预见的合格性评估的一部分进行评估。因此，本条例要求的适用性不应影响相关具体的新立法框架立法下合格性评估的具体逻辑、方法或一般结构。
(64) 鉴于高风险人工智能系统的复杂性和与之相关的风险，有必要为涉及公告机构的高风险人工智能系统制定一套适当的合格性评估程序，即所谓的第三方合格性评估。然而，鉴于专业的上市前认证机构目前在产品安全领域的经验，以及所涉及风险的不同性质，至少在本条例实施的初期阶段，限制第三方合格性评估对与产品无关的高风险人工智能系统的适用范围是适当的。因此，作为一般规则，此类系统的合格性评估应由提供者自行负责进行，唯一的例外是意图用于生物识别的人工智能系统。
(65) 为了在需要时进行第三方合格性评估，国家主管机关应根据本条例对通知机构加以通知，条件是这些机构符合一系列要求，特别是独立性、能力、无利益冲突和适当的网络安全要求。国家主管机关应通过委员会根据768/2008号决定第23条开发和管理的电子通知工具，向委员会和其他成员国发送这些机构的通知。
(65a) 根据欧盟在世界贸易组织《技术性贸易壁垒协定》中所作的承诺，只要根据第三国法律设立的合格性评估机构符合本条例的适用要求，且欧盟已就此缔结协定，就足以促进相互承认合格性评估机构所产生的合格性评估结果，而不论这些机构设立在哪一领土。为此，欧盟委员会应积极探索可能的国际文件，特别是与第三国缔结相互承认协议。

(66) 根据欧盟统一立法对产品进行实质性修改的公认概念，只要发生可能影响高风险人工智能系统遵守本条例的变化，如操作系统或软件结构的变化，或系统的预期目的发生变化，该人工智能系统就应被视为新的人工智能系统，应进行新的合格性评估。但是，如果人工智能系统在投放市场或投入使用后继续“学习”（即自动适配功能的执行方式），其算法和性能发生的变化不应构成实质性修改，前提是这些变化已由提供者预先确定，并在进行合格性评估时进行了评估。

(67) 高风险人工智能系统应带有CE标志，以表明其符合本条例，从而可在内部市场自由流动。对于嵌入产品中的高风险人工智能系统，应贴上物理CE标志，并可辅以数字CE标志。对于仅以数字方式提供的高风险人工智能系统，应使用数字CE标志。成员国不得对符合本条例规定并带有CE标志的高风险人工智能系统的市场投放或投入使用设置不合理的障碍。

(68) 在特定的情况下，快速获得创新技术可能对人的健康和安全、保护环境和气候变化以及整个社会至关重要。因此，在公共安全或保护自然人的生命和健康、环境保护以及保护关键工业和基础设施资产的特殊情况下，市场监督管理机关可以授权将未经合格性评估的人工智能系统投放市场或投入使用。在本条例规定的有正当理由的情况下，执法机关或公安机关可以不经市场监督管理机关授权而将特定的高风险人工智能系统投入使用，但必须在使用期间或使用之后申请授权，不得无故拖延。

(69) 为了促进欧盟委员会和成员国在人工智能领域的工作，并提高对公众的透明度，应要求高风险人工智能系统的提供者，与欧盟现有相关统一立法范围内的产品有关的系统除外，以及认为附件三中提到的因克减而不属于高风险的人工智能系统的提供者，在欧盟委员会建立和管理的欧盟数据库中登记自己和有关其人工智能系统的信息。在使用附件三所列的高风险人工智能系统之前，身为公共机关、机构或团体的高风险人工智能系统部署者应在该数据库中登记，并选择他们意图使用的系统。其他部署者应有权自愿如此行事。数据库的这一部分应免费向公众开放，信息应易于浏览、理解和机器可读。数据库还应方便用户使用，例如提供搜索功能，包括通过关键词，使公众能够找到附件八所列的相关信息以及高风险人工智能系统所对应的附件三所列风险领域的相关信息。对高风险人工智能系统的任何实质性修改也应在欧盟数据库中登记。对于执法、移民、庇护和边境管制管理领域的高风险人工智能系统，应在数据库的安全非公开部分履行登记义务。对安全非公开部分的访问应严格限制于欧盟委员会以及市场监督管理机关对其国家数据库部分的访问。关键基础设施领域的高风险人工智能系统只能在国家一级登记。根据欧洲议会和欧盟理事会2018/1725号条例[26]，欧盟委员会应是欧盟数据库的控制者。为确保数据库在部署后能充分发挥功能，建立数据库的程序应包括由欧盟委制定功能规范和独立审计报告。欧盟委在作为欧盟数据库的数据控制者执行任务时，应考虑网络安全和与危险有关的风险。为了最大限度地向公众提供和使用数据库，数据库，包括通过数据库提供的信息，应符合2019/882号指令的要求。

(70) 特定的旨在与自然人互动或生成内容的人工智能系统，无论是否符合高风险的条件，都可能带来假冒或欺骗的具体风险。因此，在特定的情况下，这些

[26] 欧洲议会和欧盟理事会 2016 年 4 月 27 日关于在个人数据处理方面保护自然人以及关于此类数据自由流动的 2016/679 号条例，废除 95/46/EC 号指令（《通用数据保护条例》）（官方公报，L 119，2016 年 5 月 4 日，第 1 页）。

系统的使用应遵守具体的透明度义务，同时不影响对高风险人工智能系统的要求和义务，并应考虑到执法的特殊需要，遵守有针对性的例外规定。特别是，自然人应被告知他们正在与人工智能系统互动，除非从自然人的角度来看，这一点是显而易见的，因为考虑使用的情况和场景，自然人有合理的充分知情权、观察力和谨慎性。在履行这项义务时，应考虑到因年龄或残疾而属于弱势群体的个人的特点，只要人工智能系统也意图与这些群体互动。此外，如果系统通过处理自然人的生物识别数据，能够识别或推断出这些人的情绪或意图，或将其归入特定类别，则应通知自然人。这些特定类别可能涉及性别、年龄、发色、眼色、纹身、个人特征、民族血统、个人喜好和兴趣等方面。此类信息和通知应以无障碍的格式提供给残疾人。

(70a) 各种人工智能系统可以生成大量的合成内容，而人类越来越难以将这些内容与人类生成的真实内容区分开来。这些系统的广泛可用性和日益增强的能力对信息生态系统的完整性和信任度产生了重大影响，引发了大规模的误导和操纵、欺诈、冒名顶替和欺骗消费者等新风险。鉴于这些影响、快速的技术发展以及对追踪信息来源的新方法和技术的需求，应当要求这些系统的提供者嵌入技术解决方案，以便能够以机器可读的格式进行标记，并检测出输出是由人工智能系统而非人类生成或操纵的。在技术可行的情况下，这些技术和方法应当足够可靠、可互操作、有效和稳健，同时考虑到现有的技术或这些技术的组合，如水印、元数据识别、证明内容出处和真实性的加密方法、日志记录方法、指纹或其他适当的技术。在履行这一义务时，提供者还应考虑到不同类型内容的特殊性和局限性，以及该领域的相关技术和市场发展情况，以及如同公认的先进技术水平所反映的那样，这些技术和方法是否可以在系统层面或模型的层面实施，包括是否可以在生成内容的通用人工智能模型的层面实施，从而促进人工智能系统下游提供者履行这一义务。为了保持适度，可以设想这一标识义务不应涵盖主要为标准的编辑提供辅助功能的人工智能系统，或不对部署者提供的输入数据或其语义进行实质性改变的人工智能系统。

(70b) 除系统提供者采用的技术解决方案外，使用人工智能系统生成或处理与现有人物、地点或事件明显相似的图像、音频或视频内容，并使人误以为是真实的（“深度伪造”）的部署者、遵守这一透明度义务不应被解释为使用该系统或其输出会妨碍《宪章》所保障的表达自由权和艺术与科学自由权、特别是当内容属于明显具有创造性、讽刺性、艺术性或虚构性的作品或节目的一部分时，但须适当保障第三方的权利和自由。在这些情况下，本条例规定的深度伪造的透明度义务仅限于以适当方式披露此类生成或篡改内容的存在，不妨碍作品的展示或欣赏，包括作品的正常开发和使用，同时保持作品的实用性和质量。此外，对于人工智能生成或篡改的文本，如果其发布的目的是为了向公众提供有关公共利益问题的信息，也应承担类似的披露义务，除非人工智能生成的内容经过了人工审查或编辑控制过程，而且自然人或法人对内容的发布负有编辑责任。

(70c) 为确保连贯一致的执法，应授权欧盟委员会通过执行法案，实施关于人工生成或篡改内容的标识和检测的规定。在不影响这些义务的强制性质和全面适用性的情况下，委员会还可以鼓励和促进在联盟一级起草行为守则，以促进有效履行有关检测和标注人工生成或操纵内容的义务，包括支持做出实际安排，酌情使检测机制便于使用，并促进与价值链中其他行为者的合作，传播内容或检查其真实性和来源，使公众能够有效区分人工智能生成的内容。

(70d) 本条例规定某些人工智能系统的提供者和部署者有义务能够检测和披露这些系统的输出是人为生成或操纵的，这与促进有效实施2022/2065号条例特别相关。这尤其适用于超大型在线平台或超大型在线搜索引擎提供者的义务，即识别和降低因传播人工生成或操纵的内容而可能产生的系统性风险，特别是对民主进程、公民言论和选举进程产生实际或可预见的负面影响的风险，包括通过虚假信息产生的风险。根据本条例对人工智能系统生成的内容进行标注的要求，不影响2022/2065号条例第16条第6款规定的托管服务提供者处理根据第16条第1款收到的非法内容通知的义务，也不应影响对具体内容非法性的评估和决定。该评估应完全参照有关内容合法性的规则进行。
(70e) 遵守本条例规定的人工智能系统的透明度义务不应被解释为表明根据本条例或其他联盟和成员国法律使用该系统或其输出是合法的，并且不应影响联盟或国家法律规定的人工智能系统部署者的其他透明度义务。
(71) 人工智能是一系列迅速发展的技术，需要监管监督和安全受控的实验空间，同时确保负责任的创新，并纳入适当的保障和风险缓解措施。为确保法律框架能促进创新、面向未来并能抵御干扰，成员国应确保其国家主管机关在国家一级建立至少一个人工智能监管沙盒，以促进在严格的监管监督下开发和测试创新的人工智能系统，然后再将这些系统投放市场或以其他方式投入使用。成员国也可通过参与现有监管沙盒或与一个或多个成员国主管机关联合建立沙盒来履行这一义务，只要这种参与能为参与的成员国提供同等水平的国家覆盖。监管沙盒可以以实物、数字或混合形式建立，既可容纳实物产品，也可容纳数字产品。建立机构还应确保监管沙盒有足够的资源，包括财力和人力。
(72) 人工智能监管沙盒的目标应是通过在开发和上市前阶段建立受控实验和测试环境来促进人工智能创新，以确保创新的人工智能系统符合本条例和其他相关的欧盟和成员国立法；通过监管沙盒，加强创新者的法律确定性，加强主管机关对人工智能使用的机遇、新风险和影响的监督和理解，促进机关和公司的监管学习，包括着眼于法律框架的未来调整，支持与参与人工智能监管沙盒的机关合作和分享最佳实践，并加快市场准入，包括消除对小微型企业，包括初创企业的障碍。监管沙盒应在整个欧盟范围内广泛使用，并应特别关注包括初创企业在内的小微型企业对监管沙盒的可及性。参与人工智能监管沙盒应重点关注那些会给提供者和潜在提供者带来法律不确定性的问题，以便在联盟内进行人工智能创新和实验，并促进循证的监管学习。因此，对人工智能监管沙盒中的人工智能系统的监管应涵盖系统投放市场或投入使用前的开发、培训、测试和验证，以及可能需要新的合格性评估程序的实质性修改的概念和发生。在此类人工智能系统的开发和测试过程中发现的任何重大风险，都应加以适当的缓解，如果做不到这一点，则应暂停开发和测试过程。在适当的情况下，建立人工智能监管沙盒的国家主管机关应与其他相关机关合作，包括监督基本权利保护的机关，并可允许人工智能生态系统中的其他参与者参与，如国家或欧洲标准化组织、通知机关、测试和实验设施、研究和实验实验室、欧洲数字创新中心以及利益相关方和公民社会组织。为确保在欧盟范围内统一实施并实现规模经济，宜制定监管沙盒实施的共同规则以及参与监管沙盒的相关机构之间的合作框架。根据本条例建立的人工智能监管沙盒不应妨碍允许建立其他沙盒以确保遵守本条例之外的其他立法。在适当情况下，负责这些其他监管沙盒的相关主管机关应考虑使用这些沙盒的好处，以确保人工智能系统符合本条例。经国家主管机关和人工智能监管沙盒参与者同意，也可在人工智能监管沙盒框架

内运行和监督真实世界条件下的测试。
(72a) 本条例应为人工智能监管沙盒中的提供者和潜在提供者提供合法性基础，使其仅在特定条件下，根据2016/679号条例第6条第4款和第9条第2款g项，以及2018/1725号条例第5、6和10条，并在不影响2016/680号指令第4条第2款和第10条的情况下，使用为其他目的收集的个人数据，在人工智能监管沙盒内开发符合公共利益的特定人工智能系统。2016/679号条例、2018/1725号条例和2016/680号指令规定的数据控制者的所有其他义务和数据主体的权利仍然适用。特别是，本条例不应提供2016/679号条例第22条第2款第b项和2018/1725号条例第24条第2款第b项所指的合法性基础。沙盒中的提供者和潜在提供者应确保采取适当的保障措施，并与主管机关合作，包括遵循主管机关的指导，迅速、真诚地采取行动，以充分降低在沙盒开发、测试和实验过程中可能出现的任何已识别的对安全、健康和基本权利的重大风险。
(72b) 为了加快附件三所列高风险人工智能系统的开发和投放市场进程，重要的是，这些系统的提供者或潜在提供者也可以受益于在真实世界条件下测试这些系统的具体制度，而无需参与人工智能监管沙盒。然而，在这种情况下，考虑到此类测试可能对个人造成的后果，应确保本条例为提供者或潜在提供者引入适当和充分的保障和条件。除其他外，这些保障应包括要求自然人在知情同意的情况下参与真实世界条件下的测试，但执法部门除外，因为在这种情况下征求知情同意会妨碍人工智能系统的测试。根据本条例，主体对参与此类测试的同意有别于且不影响数据主体根据相关数据保护法对其个人数据处理的同意。同样重要的是，要最大限度地降低风险，并使主管机关能够进行监督，因此要求潜在提供者向市场监督主管机关提交真实世界测试计划，在欧盟范围内的数据库中的专门部分登记测试，但存在一些有限的例外情况，设定测试期限限制，要求为属于特定弱势群体的人提供额外的保障措施，以及一份书面协议，确定潜在提供者和部署者的角色和责任，并由参与真实世界测试的主管机关进行有效监督。此外，还应适当设想额外的保障措施，以确保人工智能系统的预测、建议或决定能够被有效推翻和弃置，并确保个人数据受到保护，并在主体撤回参与测试的同意时被删除，同时不损害其根据欧盟数据保护法作为数据主体的权利。在数据传输方面，还应当设想，为在真实世界条件下进行测试而收集和处理的数据只能传输到欧盟以外的第三国，前提是根据欧盟法律实施适当和适用的保障措施，特别是根据欧盟数据保护法规定的个人数据传输依据，而对于非个人数据，则应根据欧盟法律，如《数据治理法》和《数据法》，实施适当的保障措施。
(72c) 为确保人工智能带来有益于社会和环境的成果，鼓励成员国支持和促进人工智能解决方案的研究和开发，以支持有益于社会和环境的成果，例如基于人工智能的解决方案，通过分配足够的资源，包括公共和联盟资金，增加残疾人的无障碍环境，解决社会经济不平等，或实现环境目标，并在适当情况下，在符合资格和选择标准的前提下，特别考虑追求这些目标的项目。这些项目应基于人工智能开发者、不平等和非歧视、无障碍、消费者、环境和数字权利方面的专家以及学术界之间的跨学科合作原则。
(73) 为了促进和保护创新，必须特别考虑到作为人工智能系统提供者或部署者的小微型企业，包括初创企业的利益。为此，成员国应制定针对这些运营商的举措，包括提高认识和信息沟通。成员国应向在欧盟拥有登记办公室或分支机构的小微型企业，包括初创企业提供优先进入人工智能监管沙盒的机会，前提

是它们满足资格条件和选择标准，且不排除其他提供者和潜在提供者在满足相同条件和标准的情况下进入沙盒。成员国应利用现有渠道，并在适当情况下建立新的专门渠道，与小微型企业、初创企业、部署者、其他创新者以及适当情况下的地方公共机关进行沟通，通过提供指导和答复有关本条例实施的询问，在小微型企业的整个发展道路上为其提供支持。在适当情况下，这些渠道应共同协作，发挥协同作用，并确保对小微型企业，包括初创企业和部署者的指导具有一致性。此外，成员国应促进小微型企业和其他相关利益方参与标准化制定过程。此外，在指定机构确定合格性评估费用时，应考虑到小微型企业，包括初创企业的具体利益和需求。欧盟委员会应通过透明的磋商，定期评估小微型企业，包括初创企业的认证和合规成本，并与成员国合作降低这些成本。例如，与强制性文件和与机关沟通有关的翻译费用可能会对提供者和其他运营商，特别是规模较小的提供者和运营商构成重大成本。成员国应确保其确定和接受的用于相关提供者文件和与运营商沟通的语言之一，是尽可能多的跨境部署者能够广泛理解的语言。为了满足包括初创企业在内的小微型企业的特殊需求，欧盟委员会应根据人工智能委员会的要求，为本条例所涵盖的领域提供标准化模板。此外，欧盟委员会应配合成员国的努力，为所有提供者和部署者提供一个单一的信息平台，提供与本条例有关的易于使用的信息，组织适当的宣传活动，以提高对本条例所产生的义务的认识，并评估和促进与人工智能系统有关的公共采购程序中最佳实践的趋同。最近从2003/361/EC号建议书附件（第16条）所指的小型企业转变为中型企业的中型企业应当可以利用这些支持措施，因为这些新的中型企业有时可能缺乏必要的法律资源和培训，以确保正确理解和遵守相关规定。

(73a) 为了促进和保护创新，人工智能需求响应平台，欧盟委员会和成员国在国家或联盟层面实施的所有相关欧盟资助计划和项目，如数字欧洲计划、地平线欧洲计划，应酌情为实现本条例的目标做出贡献。

(74) 特别是，为了最大限度地降低因市场缺乏知识和专业技能而导致的实施风险，并促进提供者，特别是小微型企业，包括初创企业和通知机关遵守本条例规定的义务，欧盟委员会和成员国在国家或欧盟层面建立的人工智能需求平台、欧洲数字创新中心以及测试和实验设施应为本条例的实施做出贡献。在各自的使命和职权范围内，它们尤其可以向提供者和通知机关提供技术和科学支持。

(74a) 此外，考虑到一些规模很小的经营者的创新成本，为了确保成比例性，允许微型企业以简化的方式履行最昂贵的义务之一，即建立质量管理体系，这将减少这些企业的行政负担和成本，同时不影响保护水平和遵守高风险人工智能系统要求的必要性。委员会应制定指南，明确规定微型企业以这种简化方式履行质量管理体系的要素。

(75) 欧盟委员会应尽可能为根据任何相关欧盟统一立法建立或获得认可的机构、团体或实验室使用测试和实验设施提供便利，这些机构、团体或实验室应在该欧盟统一立法所涵盖的产品或器械合格性评估范围内履行任务。根据2017/745号和2017/746号条例，医疗器械领域的专家小组、专家实验室和参考实验室尤其如此。

(75a) 本条例应建立一个治理框架，既能在国家层面协调和支持本条例的实施，又能在联盟层面建设能力，并整合人工智能领域的利益相关方。本条例的有效实施和执行需要一个治理框架，以便在联盟层面协调和建立中央专业知

识。根据委员会第[……]号决定，委员会成立人工智能办公室，其任务是发展联盟在人工智能领域的专业知识和能力，并促进联盟人工智能立法的实施。成员国应为人工智能办公室的任务提供便利，以支持在联盟一级发展联盟的专门知识和能力，并加强数字单一市场的运作。此外，应设立一个由成员国代表组成的欧洲人工智能委员会、一个整合科学界的科学小组和一个咨询论坛，为在国家和联盟层面实施本条例提供利益相关方的意见。联盟专业知识和能力的发展还应包括利用现有资源和专业知识，特别是通过与在联盟一级执行其他立法的背景下建立的结构协同增效，以及与相关的欧洲高性能计算联合事业和数字欧洲计划下的人工智能测试和实验设施协同增效。

(76) 为促进本条例的顺利、有效和协调实施，应成立欧洲人工智能委员会。欧洲人工智能委员会应反映人工智能生态系统的各种利益，并由成员国代表组成。欧洲人工智能委员会应负责一系列咨询任务，包括就与本条例实施有关的事项，包括与本条例规定的要求有关的执行事项、技术规范或现行标准，发表意见、建议、咨询或提供指导，并就与人工智能有关的具体问题向欧盟委员会和成员国及其国家主管机关提供咨询。为了让成员国在指定其在欧洲人工智能委员会中的代表时有一定的灵活性，这些代表可以是属于公共实体的任何人员，其应具有相关的能力和权力，以促进国家一级的协调，并为实现欧洲人工智能委员会的任务做出贡献。欧洲人工智能委员会应设立两个常设分组，为市场监督管理机关和通知机关就分别与市场监督管理机关和通知机关有关的问题开展合作和交流提供平台。根据2019/1020号条例第30条的规定，市场监督常设分组应作为本条例的行政合作小组(ADCO)。根据2019/1020号条例第33条规定的委员会的作用和任务，欧洲人工智能委员会应通过开展市场评估或研究来支持市场监督常设分组的活动，特别是为了确定本条例中需要市场监督管理机关之间进行具体和紧急协调的方面。欧洲人工智能委员会可酌情设立其他常设或临时分组，以研究具体问题。欧洲人工智能委员会还应酌情与活跃在欧盟相关立法背景下的欧盟相关机构、专家组和网络合作，尤其包括那些活跃在欧盟数据、数字产品和服务相关法规下的机构、专家组和网络。

(76x) 为确保利益相关者参与本条例的实施和应用，应设立一个咨询论坛，为欧洲人工智能委员会和委员会提供建议和技术知识。为确保利益相关者在商业利益和非商业利益之间的多样性和平衡性，以及在商业利益类别中，小微型企业和其他企业的代表性，咨询论坛应包括工业界、初创企业、小微型企业、学术界、公民社会（包括社会合作伙伴），以及基本权利机构、欧盟网络安全局、欧洲标准化委员会（CEN）、欧洲电工标准化委员会（CENELEC）和欧洲电信标准协会（ETSI）等。

(76y) 为支持本条例的实施和执行，特别是人工智能办公室对通用人工智能模型的监测活动，应设立一个由独立专家组成的科学小组。组成科学小组的独立专家应根据人工智能领域最新的科学或技术专业知识进行遴选，并应公正、客观地执行任务，确保在执行任务和开展活动过程中获得的信息和数据的保密性。为加强有效执行本条例所需的国家能力，成员国应能够请求科学小组专家库为其执 法活动提供支持。

(76a) 为了支持充分执行人工智能系统和加强成员国的能力，应建立欧盟人工智能测试支持机构，并提供给成员国。

(77) 成员国在本条例的适用和执行方面发挥着关键作用。为此，各成员国应指定至少一个通知机关和至少一个市场监督管理机关作为国家主管机关，负责监

督本条例的适用和执行。成员国可根据本国具体的组织特点和需要，决定指定任何类型的公共实体来执行本条例所指的国家主管机关的任务。为了提高成员国的组织效率，并在成员国和欧盟层面建立与公众和其他对应方的单一联系点，每个成员国都应指定一个市场监督管理机关作为单一联系点。

(77a) 国家主管机关应独立、公正和不带偏见地行使权力，以维护其活动和任务的客观性原则，确保本条例的适用和实施。这些机构的成员应避免采取任何与其职责不符的行动，并应遵守本条例规定的保密规则。

(78) 为了确保高风险人工智能系统的提供者能够考虑到使用高风险人工智能系统的经验，以改进其系统及设计和开发过程，或及时采取任何可能的纠正行动，所有提供者都应建立后市场监测系统。在相关情况下，后市场监测应包括分析与其他人工智能系统，包括其他设备和软件，的相互作用。后市场监测不应涵盖作为执法机关的部署者的敏感操作数据。这一系统也是确保人工智能系统在投放市场或投入使用后继续“学习”可能产生的风险能够得到更有效、更及时处理的关键。在这种情况下，还应要求提供者建立一个系统，向有关机关报告因使用其人工智能系统而导致的任何严重事故，即导致死亡或严重损害健康的事故或故障、严重和不可逆转地破坏关键基础设施的管理和运行、违反旨在保护基本权利的欧盟法律规定的义务或严重破坏财产或环境。

(79) 本条例是欧盟统一立法，为确保本条例规定的要求和义务得到适当有效的执行，应全面适用2019/1020号条例建立的市场监督和产品合规制度。根据本条例指定的市场监督管理机关应拥有本条例和2019/1020号条例规定的所有执法权力，并应独立、公正、无偏见地行使权力和履行职责。虽然大多数人工智能系统不受本条例具体要求和义务的约束，但当人工智能系统出现风险时，市场监督管理机关可根据本条例对所有人工智能系统采取措施。由于属于本条例范围内的联盟机构、机关和团体的特殊性，指定欧洲数据保护监督员作为它们的主管市场监督管理机关是合适的。这不应妨碍成员国指定国家主管机关。市场监督活动不应影响被监督实体独立执行任务的能力，如果欧盟法律要求这种独立性。

(79a) 本条例不影响监督保护基本权利的欧盟法律适用情况的相关国家公共机关或机构，包括平等机构和数据保护机关的权限、任务、权力和独立性。如有任务需要，这些国家公共机关或机构还应有权查阅根据本条例创建的任何文件。应制定具体的保障程序，以确保对健康、安全和基本权利构成风险的人工智能系统进行充分和及时的执法。针对此类有风险的人工智能系统的程序应适用于有风险的高风险人工智能系统，违反本条例规定的禁止实践而投放市场、投入使用或使用的被禁系统，以及违反本条例规定的透明度要求而提供的有风险的人工智能系统。

(80) 联盟金融服务立法包括内部治理和风险管理规则和要求，这些规则和要求适用于受监管的金融机构在提供这些服务的过程中，包括当它们使用人工智能系统时。为确保统一适用和执行本条例规定的义务以及联盟金融服务立法的相关规则和要求，负责监督和执行金融服务立法的主管机关，特别是2009/138/EC号指令、2016/97号指令、2013/36/EU号指令和575/2013号条例中定义的主管机关、欧洲议会和欧盟理事会2008/48/EC号指令和2014/17/EU号指令应在其各自权限范围内指定主管机构，负责监督本条例的实施，包括市场监督活动，涉及受监管和监督的金融机构提供或使用的人工智能系统，除非成员国决定指定另一机构履行这些市场监督任务。这些主管机关应拥有本条例和关于市场监督的

2019/1020号条例规定的所有权力，以执行本条例的要求和义务，包括开展事后市场监督活动的权力，这些活动可酌情纳入相关欧盟金融服务立法规定的现有监督机制和程序。适当的设想是，在根据本条例作为市场监督管理机关行事时，负责监督根据2013/36/EU号指令受监管的信贷机构的国家机构，如果参与了根据1024/2013号理事会条例建立的单一监督机制(SSM)，则应毫不迟延地向欧洲中央银行报告在其市场监督活动过程中发现的可能与欧洲中央银行根据该条例规定的审慎监督任务有关的任何信息。为进一步加强本条例与适用于根据欧洲议会和欧盟理事会2013/36/EU号指令监管的信贷机构的规则之间的一致性，还应将提供者在风险管理、营销后监控和文件方面的部分程序性义务纳入2013/36/EU号指令规定的现有义务和程序中。为避免重叠，还应考虑对提供者的质量管理系统和高风险人工智能系统部署者的监控义务进行有限度的克减，只要这些义务适用于受2013/36/EU号指令监管的信贷机构。同样的制度应适用于2009/138/EU号指令规定的保险和再保险业务以及保险控股公司，2016/97/EU指令规定的保险中介机构，以及其他类型的金融机构，这些机构应遵守根据相关欧盟金融服务立法制定的内部治理、安排或流程要求，以确保金融部门的一致性和平等待遇。

(80-x) 对于附件三第1点所列的高风险人工智能系统，只要这些系统用于执法目的和附件三第6、7和8点所列的目的，每个市场监督管理机关都应拥有有效的调查和纠正权力，至少包括有权获取正在处理的所有个人数据和执行任务所需的所有信息。市场监督管理机关应能完全独立地行使权力。本条例对其获取敏感业务数据的任何限制，不应影响2016/680号指令赋予其的权力。本条例中关于向国家数据保护机构披露数据的任何除外规定都不应影响这些机构当前或未来超越本条例范围的权力。

(80x) 成员国的市场监督管理机关和委员会应能够提议联合活动，包括由市场监督管理机关或市场监督管理机关与委员会联合开展的联合调查，其目的是促进合规、查明不合规情况、提高认识，并针对发现在多个成员国构成严重风险的特定类别的高风险人工智能系统提供与本条例有关的指导。应根据2019/1020号条例第9条开展促进合规的联合活动。人工智能办公室应为联合调查提供协调支持。

(80y) 对于建立在通用人工智能模型基础上的人工智能系统，有必要明确国家和联盟一级的责任和权限。为避免权限重叠，如果人工智能系统基于通用人工智能模型，且模型和系统由同一提供者提供，则应在欧盟层面通过人工智能办公室进行监管，为此，该办公室应拥有2019/1020号条例所指的市场监督管理机关的权力。在所有其他情况下，国家市场监督管理机关仍负责人工智能系统的监管。然而，对于部署者可直接用于至少一个被归类为高风险的目的的通用人工智能系统，市场监督管理机关应与人工智能办公室合作，对合规性进行评估，并相应地通知欧洲人工智能委员会和其他市场监督管理机关。此外，如果市场监督管理机关因无法获得与高风险人工智能系统所基于的通用人工智能模型相关的某些信息而无法完成对高风险人工智能系统的调查，市场监督管理机关应能够请求人工智能办公室提供协助。在这种情况下，应类推适用2019/1020号条例第六章中关于跨境案件互助的程序。

(80z) 为了最好地利用集中的联盟专门知识和联盟一级的协同作用，对通用人工智能模型提供者的义务进行监督和执行的权力应该是委员会的职权。委员会应委托人工智能办公室执行这些任务，同时不影响委员会的组织权力以及成员

国和联盟之间基于条约的权限划分。人工智能办公室应能采取一切必要行动，监督本条例在通用人工智能模型方面的有效实施。它应能根据其监测活动的结果，或应市场监督管理机关的要求，按照本条例规定的条件，主动调查可能违反有关通用人工智能模型提供者规则的行为。为支持对人工智能办公室进行有效监督，应规定下游提供者可就可能违反通用人工智能系统提供者规则的行为提出投诉。

(80z+1) 为了补充通用人工智能模型的治理系统，科学小组应支持人工智能办公室的监测活动，并可在特定情况下向人工智能办公室发出有条件的警报，从而触发调查等后续行动。如果科学小组有理由怀疑通用人工智能模型在联盟一级构成具体且可识别的风险，就应该这样做。此外，当科学小组有理由怀疑一个通用人工智能模型符合可导致被归类为具有系统性风险的通用人工智能模型的标准时，也应属于这种情况。为了使科学小组具备执行这些任务所需的信息，应建立一个机制，使科学小组能够要求委员会要求提供者提供文件或信息。

(80z+2) 人工智能办公室应能采取必要行动，监督本条例规定的通用人工智能模型提供者义务的有效实施和遵守情况。人工智能办公室应能根据本条例规定的权力调查可能的违规行为，包括要求提供文件和信息，进行评估，以及要求通用人工智能模型提供者采取措施。在进行评估时，为了利用独立的专业知识，人工智能办公室应能够让独立专家代表其进行评估。应通过要求采取适当措施，包括在发现系统性风险的情况下采取风险缓解措施，以及限制在市场上提供、撤回或召回模型等方式，强制履行这些义务。作为本条例规定的程序性权利之外所需的保障措施，通用人工智能模型的提供者应享有2019/1020号条例第18条规定的程序性权利，该权利应以类推方式适用，但不影响本条例规定的更具体的程序性权利。[27]

(81) 按照本条例的要求开发高风险人工智能系统以外的其他人工智能系统，可能导致在欧盟更多地采用合乎道德和值得信赖的人工智能。应鼓励非高风险人工智能系统的提供者制定行为守则，包括相关的治理机制，以促进自愿适用适用于高风险人工智能系统的部分或全部强制性要求，这些要求应根据系统的预期目的和所涉及的较低风险进行调整，并考虑到可用的技术解决方案和行业最佳实践，如模型卡和数据卡。还应鼓励所有人工智能系统，无论是否高风险的提供者和模型的提供者，并酌情鼓励其部署者，在自愿的基础上适用与欧洲可信人工智能伦理准则要素、环境可持续性、人工智能素养措施、人工智能系统的包容性和多样化设计与开发等有关的额外要求、在设计和开发人工智能系统时，酌情让利益相关方，如企业和公民社会组织、学术和研究组织、工会和消费者保护组织，参与进来，以及开发团队的多样性，包括性别平衡。为确保自愿行为守则行之有效，守则应基于明确的目标和关键绩效指标，以衡量这些目标的实现情况。在制定守则时，应酌情让有关各方参与，例如商界和公民社会组织、学术界和研究机构、工会和消费者保护组织。委员会可制定包括部门性质在内的倡议，以促进降低阻碍跨境交换数据以促进人工智能发展的技术壁垒，包括数据访问基础设施、不同类型数据的语义和技术互操作性。

(82) 重要的是，根据本条例不属于高风险的与产品有关人工智能系统，因而不

[27] 欧洲议会和理事会 2013 年 6 月 26 日关于信贷机构活动准入以及信贷机构和投资公司审慎监管的 2013/36/EU 号指令，修订 2002/87/EC 号指令，并废除 2006/48/EC 号和 2006/49/EC 号指令（官方公报，L 176，2013 年 6 月 27 日，第 338 页）。

需要遵守为高风险人工智能系统规定的要求，尽管如此，在投放市场或投入使用时仍然应是安全的。为促进实现这一目标，欧洲议会和欧盟理事会2023/988号条例[28]将作为安全网适用。

(83) 为确保联盟和国家主管机关之间的信任和建设性合作，参与实施本条例的各方应根据联盟或国家法律，尊重在执行任务过程中获得的信息和数据的机密性。他们在执行任务和开展活动时，应特别保护知识产权、商业机密信息和商业秘密、本条例的有效实施、公共和国家安全利益、刑事或行政诉讼程序的完整性以及机密信息的完整性。

(84) 应通过实施处罚和其他执行措施来强制遵守本条例。成员国应采取一切必要措施，确保本条例的规定得到执行，包括对违反本条例的行为规定有效、适度且阻遏性的处罚，并遵守一事不再理原则。为了加强和统一对违反本条例行为的行政处罚，应规定对特定的违法行为的行政罚款上限。在评估罚款金额时，成员国应根据具体情况考虑所有相关情况，尤其应适当考虑侵权行为及其后果的性质、严重程度和持续时间，以及提供者的规模，特别是如果提供者是小微型企业，包括初创企业。欧洲数据保护监督员应有权对本条例范围内的联盟机构、机关和团体处以罚款。

(84a) 本条例对通用人工智能模型提供者规定的义务应通过罚款等方式强制执行。为此，还应对违反这些义务的行为规定适当的罚款额度，包括不遵守委员会根据本条例要求采取的措施，并根据成比例性原则规定适当的时效期限。欧盟委员会根据本条例做出的所有决定都将根据《欧洲联盟运作条约》接受欧盟法院的审查。

(84aa)欧盟和国内法律已经为权利和自由受到使用人工智能系统不利影响的自然人和法人提供了有效的补救措施。在不影响这些补救措施的前提下，任何有理由认为本条例的规定遭到违反的自然人或法人都有权向相关市场监督管理机关提出申诉。

(84b) 当部署者以本条例规定的特定的高风险系统的输出结果为主要依据做出决定，并对其产生法律效力或类似的重大影响，而受影响者认为该决定对其健康、安全或基本权利产生不利影响时，受影响者应有权要求解释。这种解释应明确而有意义，并应为受影响者行使其权利提供依据。这不应适用于欧盟或国家法律规定了例外或限制的人工智能系统的使用，并且仅适用于欧盟法律尚未规定的权利。

(84c) 作为违反本条例行为的“吹哨人”，应得到关于保护违法行为举报者的欧盟立法所保障的保护。因此，2019/1937号指令应适用于对违反本条例行为的举报以及对举报者的保护。

(85) 为了确保必要时可以调整管理框架，应授权委员会根据《欧洲联盟运作条约》第290条通过法案，以修订附件二所列的欧盟统一立法、附件三中所列的高风险人工智能系统、附件四中所列的有关技术文件的规定、附件五中欧盟合格性声明的内容、附件六和七中有关合格性评估程序的规定、建立高风险人工智能系统的规定，基于质量管理系统评估和技术文件评估的合格性评估程序应适用于这些系统；具有系统风险的通用人工智能模型分类规则中的阈值以及补充

[28] 欧洲议会和理事会 2023 年 5 月 10 日关于通用产品安全的 2023/988 号条例，修订欧洲议会和理事会 1025/2012 号条例以及欧洲议会和理事会 2020/1828 号指令，并废除欧洲议会和理事会 2001/95/EC 号指令以及理事会 87/357/EEC 号指令（与欧洲经济区相关的文本）（官方公报，L 135，2023 年 5 月 23 日，第 1-51 页）。

基准和指标；附件YY中具有系统风险的通用人工智能模型的指定标准；附件八b中通用人工智能模型提供者的技术文件；附件八c中通用人工智能模型提供者的透明度信息。特别重要的是，委员会应在筹备工作中开展适当的磋商，包括专家层面的磋商，并按照2016年4月13日《关于更好地制定法律的机构间协议》中规定的原则开展这些磋商。特别是，为确保平等参与授权法案的准备工作，欧洲议会和欧盟理事会与成员国专家同时收到所有文件，其专家有系统地参加欧盟委专家小组关于准备授权法案的会议。

(85a) 鉴于技术的快速发展以及有效实施本条例所需的专业技术知识，欧盟委员会应在本条例生效之日起三年后对其进行评估和审查，此后每四年评估和审查一次，并向欧洲议会和理事会报告。此外，考虑到对本条例适用范围的影响，欧盟委员会应每年评估一次修订附件三清单和禁止行为清单的必要性。此外，在本条例生效后两年内，以及此后每四年，委员会应评估并向欧洲议会和欧盟理事会报告是否有必要修订附件三中的高风险领域、第四章透明度义务范围内的人工智能系统、监督和治理系统的有效性，以及关于通用人工智能模型节能开发的标准化可交付成果的开发进度，包括是否有必要采取进一步措施或行动。最后，在生效后两年内，以及此后每三年，委员会应评估自愿行为守则的影响和有效性，以促进高风险人工智能系统以外的系统应用第三篇第二章中的要求，以及可能对此类人工智能系统的其他额外要求。

(86) 为确保本条例实施条件的统一，应赋予欧盟委员会实施权力。这些权力应根据欧洲议会和欧盟理事会182/2011号条例行使。

(87) 由于成员国无法充分实现本条例的目标，而且由于行动的规模或效果，在欧盟一级可以更好地实现该目标，因此联盟可根据《欧洲联盟运作条约》第5条规定的辅助性原则采取措施。根据该条规定的成比例性原则，本条例不超越实现该目标所必需的范围。

(87a) 为了确保法律的确定性，确保经营者有一个适当的适应期，并避免对市场的干扰，包括确保人工智能系统使用的连续性，本条例适用于在其一般适用日期之前已投放市场或投入使用的高风险人工智能系统，仅当从该适用日期起，这些系统的设计或预期目的经历了重大改变。需要说明的是，在这方面，重大改变的概念应被理解为实质上等同于实质性修改的概念，后者仅用于本条例所定义的高风险人工智能系统。作为例外情况，并考虑到公共责任，作为附件九所列法案建立的大型信息技术系统组成部分的人工智能系统的运营商，以及意图由公共机关使用的高风险人工智能系统的运营商，应采取必要步骤，分别在2030年底前和生效后四年内遵守本条例的要求。

(87b) 鼓励高风险人工智能系统的提供者在过渡期内就开始自愿遵守本条例规定的相关义务。

(88) 本条例应自[……]起适用。然而，考虑到与以特定方式使用人工智能有关的不可接受的风险，禁止规定应从本条例生效后6个月开始适用。虽然这些禁止规定的全部效力将随着本条例的管理和执行的建立而发生，但对禁止规定适用的期待对于考虑不可接受的风险非常重要，并对其他程序产生影响，如民法中的程序。此外，与管理和合格性评估系统有关的基础设施应在该日期之前投入使用，因此，关于通知机关和管理结构的规定应自本条例生效后十二个月起适用。鉴于技术进步和采用通用人工智能模型的速度很快，通用人工智能模型提供者的义务应在本条例生效之日起12个月内适用。行为守则最迟应在相关规定生效前3个月准备就绪，以便提供者能够及时证明遵守了规定。人工智能办公室

应确保分类规则和程序与技术发展同步。此外，各成员国应制定处罚规则，包括行政罚款，并通知欧盟委员会，确保在本条例生效之日前得到适当有效的执行。因此，有关处罚的规定应在本条例生效后十二个月内适用。
(89) 根据2018/1725号条例第42条第2款，与欧洲数据保护监督员和欧洲数据保护委员会进行了磋商，并于2021年6月18日发表了意见。

已经通过了该条例：

第一编

第1条
主题

(1) 本条例的目的是改善内部市场的运作，促进以人为本、值得信赖的人工智能的应用，同时确保对健康、安全、《宪章》规定的基本权利，包括民主、法治和环境保护，的高度保护，使其免受联盟内的人工智能系统的有害影响，并支持创新。
本条例规定了：
(a) 关于人工智能系统在欧盟的市场投放、投入使用和使用的统一规则；
(b) 禁止特定的人工智能实践；
(c) 对高风险人工智能系统的具体要求以及此类系统运营商的义务；
(d) 特定人工智能系统的统一透明度规则；
(da) 通用人工智能模型投放市场的统一规则；
(e) 关于市场监测、市场监督治理和执法的规则；
(ea) 支持创新的措施，重点是小微型企业，包括初创企业；

第2条
范围

1. 本条例适用于：
(a) 在欧盟境内将人工智能系统投放市场或投入使用或将通用人工智能模型投放市场的提供者，无论这些提供者是设立于，还是位于欧盟境内或者第三国；
(b) 在联盟内设立场所或者位于联盟内的人工智能系统部署者；
(c) 场所位于第三国或者位于第三国的人工智能系统提供者和部署者，其系统产生的产出用于欧盟；
(ca) 人工智能系统的进口者和分销者；
(cb) 产品制造商以自己的名称或商标将人工智能系统与其产品一起投放市场或投入使用；
(cc) 未在欧盟境内设立的提供者的授权代表。
(cc) 位于联盟内的受影响者。
2. 对于根据第6条第1款和第6条第2款被列为高风险人工智能系统的、与附件二第B节所列欧盟统一立法涵盖的产品有关的人工智能系统，仅适用本条例第84条。第53条仅在本条例对高风险人工智能系统的要求已纳入欧盟统一立法的情况下适用。

3. 本条例不适用于欧盟法律范围之外的领域，在任何情况下都不得影响成员国在国家安全方面的权限，无论成员国委托哪一类实体执行与这些权限有关的任务。
本条例不适用于专门为军事、国防或国家安全目的而投放市场、投入使用或经修改或不经修改而使用的人工智能系统，无论从事这些活动的实体属于何种类型。
本条例不适用于未在欧盟投放市场或投入使用的人工智能系统，如果其产出在欧盟仅用于军事、国防或国家安全目的，则无论开展这些活动的实体属于何种类型。
4. 本条例不适用于根据第1款属于本条例范围内的第三国公共机关或国际组织，如果这些机关或组织在与欧盟或一个或多个成员国进行执法和司法合作的国际合作或协议框架内使用人工智能系统，条件是该第三国或国际组织在保护个人基本权利和自由方面提供充分保障；
5. 本条例不影响欧洲议会和欧盟理事会2000/31/EC号指令第二章第4节中有关中介服务提供者责任的规定的适用。[29]
5a. 本条例不适用于专为科学研究和开发目的而开发和投入使用的人工智能系统和模型，包括其输出。
5a. 关于保护个人数据、隐私和通信保密的欧盟法律适用于与本条例规定的权利和义务有关的个人数据处理。在不影响本条例第10条第5款和第54条规定的安排的情况下，本条例不影响2016/679 和2018/1725 号条例以及2002/58/EC和2016/680号指令；
5b. 本条例不适用于人工智能系统或模型在投放市场或投入使用前的任何研究、测试和开发活动；这些活动的开展应遵守适用的欧盟法律。在真实世界条件下进行的测试不在此豁免范围内。
5b. 本条例不妨碍与消费者保护和产品安全相关的其他欧盟法案所规定的规则。
5c. 本条例不适用于在纯粹个人非职业活动中使用人工智能系统的自然人部署者的义务。
5e. 本条例不妨碍成员国或欧盟保留或引入在雇主使用人工智能系统方面更有利于保护工人权利的法律、法规或行政规定，或鼓励或允许适用更有利于工人的集体协议。
5g. 本条例规定的义务不适用于根据免费且开源许可发布的人工智能系统，除非这些系统作为高风险人工智能系统或属于第二编和第四编的人工智能系统投放市场或投入使用。

第3条
定义

(1) 人工智能系统是一种基于机器的系统，设计为以不同程度的自主性运行，在部署后可能表现出适应性，并且为了明确或隐含的目标，从其接收的输入中推断如何生成可影响物理或虚拟环境的输出，如预测、内容、建议或决定；
(1a) “风险”是指发生危害的可能性和危害的严重性的组合；
(2) “提供者”是指开发人工智能系统或通用人工智能模型，或已开发人工智

[29] 欧洲议会和理事会 2000 年 6 月 8 日关于内部市场信息社会服务，特别是电子商务的若干法律问题的 2000/31/EC 号指令（《电子商务指令》）（官方公报，L 178，2000 年 7 月 17 日，第 1 页）。

能系统或通用人工智能模型，并将其投放市场或以自己的名义或商标投入使用的自然人或法人、公共机关、机构或其他团体，无论有偿还是无偿；
(4) 部署者是指在其授权下使用人工智能系统的任何自然人或法人、公共机关、机构或其他团体，但在个人非职业活动中使用人工智能系统的情况除外；
(5) “授权代表”是指位于或设立在欧盟的任何自然人或法人，他们接受了人工智能系统或通用人工智能模型提供者的书面授权，分别代表其履行和执行本条例规定的义务和程序；
(6) “进口者”是指位于或设立于欧盟的任何自然人或法人，将带有在欧盟以外设立的自然人或法人的名称或商标的人工智能系统投放市场；
(7) “分销者”是指供应链中除提供者或进口者之外，在欧盟市场上提供人工智能系统的任何自然人或法人；
(8) “经营者”指提供者、产品制造商、部署者、授权代表、进口者或分销者；
(9) “投放市场”是指在欧盟市场上首次提供人工智能系统或通用人工智能模型；
(10) “在市场上提供”是指在商业活动中提供人工智能系统或通用人工智能模型，供在联盟市场上销售或使用，无论有偿还是无偿；
(11) “投入使用”是指将人工智能系统直接提供给部署者首次使用，或供其在联盟内按预定目的自用；
(12) “预期目的”是指提供者在使用说明、宣传或销售材料和声明以及技术文件中 提供的信息所规定的人工智能系统的预期用途，包括具体的使用环境和条件；
(13) “可合理预见的误用”是指人工智能系统的使用方式与其预期目的不符，但可能是由可合理预见的人类行为或与其他系统，包括其他人工智能系统，的互动造成的；
(14) “产品或系统的安全组件”是指产品或系统的一个组件，该组件对该产品或系统具有安全功能，或其故障或失灵危及人或财产的健康和安全；
(15) “使用说明”是指提供者特别为告知用户人工智能系统的预期目的和正确使用 而提供的信息；
(16) “人工智能系统的召回”是指任何旨在实现向提供者返还或使其停止服务或禁止使用提供给部署者的人工智能系统的措施；
(17) “撤回人工智能系统”是指任何旨在阻止供应链中的人工智能系统在市场上销售的措施；
(18) “人工智能系统的性能”是指人工智能系统实现其预期目的的能力；
(19) “通知机关”是指负责制定和实施评估、指定和通知合格性评估机构及其监督的必要程序的国家机关；
(20) “合格性评估”是指证明本条例第三编第二章中有关高风险人工智能系统的要求是否得到满足的过程；
(21) “合格性评估机构”指进行第三方合格性评估活动的机构，包括测试、认证和检验；
(23) “实质性修改”是指人工智能系统在投放市场或投入使用后发生的修改，这种修改在提供者最初的合格性评估中没有预见到或没有计划，并因此影响人工智能系统符合本条例第三遍第二章规定的要求，或导致人工智能系统被评估的预期目的发生修改；

(24) “CE合格性标识”（CE标识）是指一种标识，提供者通过该标识表明人工智能系统符合本条例第三编第二章中规定的要求，以及统一规定产品贴标销售的条件的其他适用的欧盟立法（“欧盟统一立法”）；
(25) “后市场监测系统”是指人工智能系统提供者为收集和审查从使用其投放市场或投入使用的人工智能系统中获得的经验而开展的所有活动，目的是确定是否需要立即采取任何必要的纠正或预防措施；
(26) “市场监督管理机关”指根据2019/1020号条例开展活动和采取措施的国家机关；
(27) “统一标准”是指1025/2012号条例第2条第1款第c项定义的欧洲标准；
(28) “共同规格”是指1025/2012号条例第2条第4款定义的一套技术规格，该规格提供了遵守本条例规定的特定要求的方法；
(29) “训练数据”指通过拟合可学习的参数来训练人工智能系统的数据；
(30) “验证数据”是指用于对经过训练的人工智能系统进行评估、调整其不可学习参数和学习过程等的数据，以防止欠拟合或过拟合；验证数据集可以是一个单独的数据集，也可以是训练数据集的一部分，以固定或可变的方式加以切分；
(31) “测试数据”是指用于对人工智能系统进行独立评估的数据，以确认该系统在投放市场或投入使用前的预期性能；
(32) “输入数据”是指提供给人工智能系统或由人工智能系统直接获取的数据，系统根据这些数据产生输出；
(33) “生物识别数据”系指与自然人的身体、生理或行为特征有关的由特定技术处理所产生的个人数据，如面部图像或指纹和掌纹数据；
(33a) “生物识别 ”是指自动识别人的身体、生理、行为和心理特征，通过将该人的生物识别数据与数据库中存储的个人生物识别数据进行比较，从而确认该人的身份；
(33c) “生物验证”是指通过将个人的生物识别数据与之前提供的生物识别数据进行比较，自动验证自然人的身份（一对一验证，包括鉴别）；
(33d) “特殊类别个人数据”是指2016/679号条例第9条第1款、2016/680号指令第10条和2018/1725号条例第10条第1款中提及的个人数据类别；
(33e) “敏感业务数据”是指与预防、侦查、调查和起诉刑事犯罪活动有关的业务数据， 披露这些数据会损害刑事诉讼程序的整全性。
(34) “情感识别系统”指根据自然人的生物识别数据识别或推断其情感或意图的人工智能系统；
(35) “生物识别分类系统”是指根据自然人的生物识别数据将其归入特定类别的人工智能系统，除非该系统附属于另一项商业服务，且因客观技术原因而严格必要；
(36) “远程生物识别系统”系指一种人工智能系统，其目的是在没有自然人主动参 与的情况下，通常通过将一个人的生物识别数据与参考数据库中的生物识别数 据进行比较，远距离识别自然人的身份；
(37) “‘实时’远程生物识别系统”是指一种远程生物鉴别系统，在该系统中，生物识别数据的采集、比较和识别都是在没有明显延迟的情况下进行的。这不仅包括即时识别，还包括有限的短暂延迟，以避免规避本条例；
(38) “‘事后’远程生物识别系统”指“实时”远程生物识别系统之外的远程生物识别系统；

(39) “公众可进入的场所”是指任何公有或私有的、可供人数不确定的自然人进入的有形场所，不论是否适用特定的进入条件，也不论潜在的容量限制；
(40) “执法机关”是指：
(a) 任何主管预防、调查、侦查或起诉刑事犯罪或执行刑事处罚，包括保障和预防对公共安全的威胁的公共机关；或
(b) 受成员国法律委托，为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚，包括保障和预防对公共安全的威胁而行使公共权力的任何其他机构或实体；
(41) “执法”指执法机关或代表执法机关为预防、调查、侦查或起诉刑事犯罪或执行刑罚而开展的活动，包括保障和预防对公共安全的威胁；
(42) 人工智能办公室指委员会促进人工智能系统的实施、监测和监督以及人工智能治理的职能。本条例中对人工智能办公室的提及，应理解为提及委员会。
(43) “国家主管机关”指以下任何一方：通知机关和市场监督管理机关。关于欧盟机构、机关、办公室和团体投入使用或使用的人工智能系统，本条例中提及的国家主管机关或市场监督管理机关应理解为指欧洲数据保护监督员；
(44) “严重事故”是指直接或间接导致以下任何情况的人工智能系统事故或故障：
(a) 致人死亡或严重损害人的健康；
(b) 严重和不可逆转地破坏重要基础设施的管理和运行；
(ba) 违反旨在保护基本权利的联盟法律规定的义务
(bb) 对财产或环境造成严重损害。
(44a) “个人数据”是指2016/679号条例第4条第1点所定义的个人数据；
(44c) “非个人数据”指2016/679号条例第4条第1点所定义的个人数据之外的数据；
(be)“画像”是指2016/679号第4条第4点所定义的任何形式的个人数据的自动化处理；或就执法机关而言——2016/680号指令第3条第4点所定义的个人数据的自动化处理；或就欧盟机构、团体、办公室或机关而言——2018/1725号条例第3条第5点所定义的个人数据的自动化处理；
(bf) “真实世界测试计划”是指描述在真实世界条件下测试的目标、方法、地理、人口和时间范围、监测、组织和开展的文件；
(44eb) “沙盒计划”是指参与提供者与主管机关之间商定的文件，其中描述了在沙盒内开展活动的目标、条件、时间框架、方法和要求。
(bg) “人工智能监管沙盒”是指由主管机关建立的一个具体和受控的框架，为人工智能系统的提供者或潜在提供者提供在监管监督下根据沙盒计划在有限的时间内开发、培训、验证和测试创新人工智能系统的可能性。
(bh) “人工智能素养”是指这样的技能、知识和理解，使提供者、使用者和受影响者在考虑到各自在本条例中的权利和义务的情况下，能够在知情的情况下部署人工智能系统，并认识到人工智能的机遇和风险以及可能造成的损害。
“真实世界条件下的测试”是指在实验室或其他模拟环境之外的实际条件下，为预期目的对人工智能系统进行的临时测试，目的是收集可靠且可信的数据，评估和验证人工智能系统是否符合本条例的要求；只要符合第53条或第54a条规定的所有条件，实际条件下的测试不应视为将人工智能系统投放市场或投入使用；
(bj) 就真实世界测试而言，“测试主体”是指在真实世界条件下参加测试的自

然人；
(bk) “知情同意”系指测试主体在被告知与测试主体决定参加的测试有关的各方面情况之后，自由、具体、明确和自愿地表示愿意在真实世界的条件下参与一项测试；
(bl) “深度伪造”是指由人工智能生成或操纵的图像、音频或视频内容，这些内容与现有的人员、物体、地点或其他实体或事件相似，会让人误以为是实在的或真实的；
(44e) “广泛侵权”是指违反保护个人利益的联盟法律的任何作为或不作为：
(a) 损害或可能损害居住在除该成员国以外的至少两个成员国的个人的集体利益，在这一成员国中
(i) 作为或不作为源起或发生；
(ii) 相关的提供者或，如适用，其授权代表设立；或
(iii) 在部署者实施侵权行为时，部署者设立；
(b) 保护个人利益，对个人集体利益造成、导致或可能造成损害，并具有共同的特征，包括同一非法行为、同一利益受到侵犯，以及由同一经营者在至少三个成员国同时实施；
(44h) “关键基础设施”是指提供2022/2557号指令第2条第4款所指的基本服务所必需的资产、设施、设备、网络或系统，或其中的一部分；
(44b) “通用人工智能模型”是指一个人工智能模型，包括在使用大量数据进行大规模自我监督训练时，无论该模型以何种方式投放市场，都显示出显著的通用性，能够胜任各种不同的任务，并可集成到各种下游系统或应用中。这不包括在投放市场前用于研究、开发和原型设计活动的人工智能模型。
(44c) 通用人工智能模型中的“高影响能力”是指与最先进的通用人工智能模型中记录的能力相匹配或超过这些能力的能力；
(44d) “联盟层面的系统性风险”是指通用人工智能模型的高影响能力所特有的风险，因其影响范围广泛而对内部市场产生重大影响，并对公众健康、安全、公共安全、基本权利或整个社会产生实际或可合理预见的负面影响，可在整个价值链中大规模传播；
(44e) “通用人工智能系统”是指以通用人工智能模型为基础的人工智能系统，该系统具有服务于各种目的的能力，既可直接使用，也可集成到其他人工智能系统中；
(44f) “浮点运算”是指涉及浮点数的任何数学运算或赋值，浮点数是实数的一个子集，在计算机上通常以固定精度的整数表示，并以固定基数的整数指数加以缩放。
(44g) “下游提供者”指集成了人工智能模型的人工智能系统，包括通用人工智能系统，的提供者，无论该模型是由其自身提供并进行垂直整合，还是由其他实体基于合同关系而提供。

第4b条
人工智能素养

2.人工智能系统的提供者和部署者应采取措施，考虑其技术知识、经验、教育和培训以及人工智能系统的使用环境，并考虑人工智能系统将用于哪些人或群体，尽最大努力确保其工作人员和代表其处理人工智能系统操作和使用的其他

人员具有足够的人工智能知识水平。

第二编
禁止的人工智能实践

第5条
禁止的人工智能实践

1. 禁止下列人工智能实践：
(a) 在市场上投放、投入使用或使用人工智能系统，该系统采用超出个人意识的潜意识技术或有目的的操纵或欺骗技术，其目的或效果是通过明显损害一个人或一群人做出知情决定的能力，实质性地扭曲该人或一群人的行为，从而导致该人做出其本来不会做出的决定，造成或可能造成对该人、另一人或一群人的重大伤害；
(b) 在市场上投放、投入使用或使用人工智能系统，利用特定个人或特定群体因其年龄、残疾或特定社会或经济状况而具有的任何弱点，以实质性扭曲该人或属于该群体的人的行为，造成或有合理可能造成该人或他人重大伤害为目的或效果；
(ba) 为这一特定目的在市场上投放或使用生物识别分类系统，根据生物识别数据对自然人进行个体层面的分类，以推导或推断其种族、政治观点、工会成员身份、宗教或哲学信仰、性生活或性取向。
这项禁令不包括根据生物识别数据对合法获取的生物识别数据集，如图像，进行标注或过滤，也不包括在执法领域对生物识别数据进行分类。
(c) 将根据自然人或其群体的社会行为或已知、推断或预测的个人或个性特征，在一定时期内对其进行评估或分类的人工智能系统投放市场、投入使用或使用，系统的社会得分可导致以下任何一种或两种情况：
(i) 在与最初生成或收集数据的场景无关的社会场景下，特定自然人或其整个群体的不利或不利待遇；
(ii) 对特定自然人或群体的有害或不利待遇，而这种待遇是不合理的，或与其社会行为或其严重性不成比例的；
(d) 在公共场所为执法目的使用“实时”远程生物鉴别系统，除非这种使用是为下列目标之一所严格必要的：
(i) 有针对性地搜寻特定的绑架、贩卖人口和性剥削受害者，以及搜寻失踪人员；
(ii) 防止对自然人的生命或人身安全构成确切、重大切紧迫的威胁，或防止真实存在或真实可预见的恐怖袭击威胁；
(iii) 为了对附件二a所述罪行进行刑事调查、起诉或执行刑事处罚，对涉嫌犯有刑事罪行的人进行定位或身份识别，而这些罪行在相关成员国可被判处监禁或最短不少于四年的拘留令。本段规定不影响《通用数据保护条例》第9条有关为执法以外目的而处理生物识别数据的规定。
(da) 在市场上投放、为此特定目的投入使用或使用人工智能系统对自然人进行风险评估，以评估或预测自然人实施刑事犯罪的风险，而这完全是基于对自然人的画像或对其个性特征和特点的评估；
这一禁令不适用于这样的人工智能系统，其根据与犯罪活动直接相关的客观且

可核实的事实，支持人类对特定个人是否参与犯罪活动的评估。
(db) 将人工智能系统投放市场、为此特定目的投入使用或使用，通过从互联网或闭路电视录像中普遍地爬取面部图像来创建或扩展面部识别数据库；
(dc) 将人工智能系统投放市场、为此特定目的投入使用，或在工作场所和教育机构领域使用人工智能系统推断自然人的情绪，但出于医疗或安全原因意图将人工智能系统投入使用或投放市场的情况除外；
1a. 本条不影响适用于人工智能实践违反其他联盟法律的禁止规定。
2. 为第1款第d项所述任何目标而在可进入的公共场所使用“实时”远程生物识别系统，只能用于第1款第d项所述的目的，以确认具体目标个人的身份，并应考虑以下因素：
(a) 导致可能使用该系统的情况的性质，特别是在不使用该系统的情况下所造成的损害的严重性、可能性和规模；
(b) 使用该系统对所有有关的人的权利和自由造成的后果，特别是这些后果的严重性、 可能性和规模。
此外，为实现第1款第d项所述的任何目标而在公众可进入的场所使用“实时”远程生物识别系统进行执法时，应根据授权使用该系统的国家法律，遵守与使用有关的必要且成比例的保障措施和条件，特别是在时间、地理和个人限制方面。
只有在执法机关完成了第29a条规定的基本权利影响评估，并根据第51条的规定在数据库中登记了该系统后，才可授权在公共场所使用“实时”远程生物识别系统。不过，在有正当理由的紧急情况下，可以不经登记就开始使用该系统，但登记工作必须在没有无故拖延的情况下完成。
3. 关于第1款第d项和第2款，在公共场所为执法目的使用“实时”远程生物识别系统，应事先得到使用该系统的成员国司法机关或独立行政机关的授权，该机关的决定对使用该系统的成员国具有约束力。但是，在有正当理由的紧急情况下，可以在没有授权的情况下开始使用该系统，但应及时申请授权，最迟不得超过24小时。如果该授权被拒绝，则应立即停止使用，并应立即弃置和删除所有数据以及使用的结果和输出。
主管司法机关或其决定具有约束力的独立行政机关只有在根据客观证据或向其提交的明确迹象，确信使用有关“实时”远程生物识别系统对实现第1款第d项所规定的目标之一是必要并成比例的时候，特别是在时间以及地理和个人范围方面仍限于严格必要的情况下，才应给予授权。主管司法机关或其决定具有约束力的独立行政机关在对申请做出决定时，应考虑第2款提及的因素。应确保司法机关或其决定具有约束力的独立行政机关不得仅根据远程生物识别系统的输出结果做出对个人产生不利法律影响的决定。
3a. 在不影响第3款的情况下，每次为执法目的在公共场所使用“实时”远程生物识别系统，均应按照第4款提及的国家规则通知有关市场监督管理机关和国家数据保护机关。通知至少应包含第5款规定的信息，不得包括敏感业务数据。
4. 成员国可在第1款第d项、第2款和第3款所列的范围和条件下，为执法目的，决定提供全部或部分授权在公共场所使用“实时”远程生物识别系统的可能性。有关成员国应在其国内法中就第3款所述授权的申请、签发、行使、监督和报告制定必要的详细规则。这些规则还应具体说明，在第1款第d项所列的目标中，包括在第3点所指的刑事犯罪中，主管机关可授权为执法目的使用这些系统。成员国最迟应在这些规则通过后30天内将其通知委员会。

成员国可根据欧盟法律，就远程生物识别系统的使用制定限制性更强的法律。
5. 成员国的国家市场监督管理机关和国家数据保护机关，如被告知根据第3a款为执法目的在可公开进入的场所使用“实时”远程生物识别系统，应向委员会提交关于此类使用情况的年度报告。为此，委员会应向成员国及国家市场监督管理机关和数据保护机关提供一个模板，其中包括主管司法机关或独立行政机关做出的对根据第3款提出的授权请求具有约束力的决定的数目及其结果的信息；
6. 委员会应根据成员国基于第5款所述年度报告的汇总数据，发布关于为执法目的在公共场所使用“实时”远程生物识别系统的年度报告，其中不应包括相关执法活动的敏感业务数据。

第三编
高风险人工智能系统

第6条
高风险人工智能系统分类规则

1. 无论人工智能系统是否独立于第a和b点所述产品投放市场或投入使用，只要满足以下两个条件，该人工智能系统就应被视为高风险系统：
(a) 人工智能系统意图用作产品的安全组件，或者人工智能系统本身就是附件二所列的欧盟统一立法所涵盖的产品；
(b) 根据第a点，其安全组件为人工智能系统的产品，或作为产品的人工智能系统本身，必须接受第三方合格性评估，以便根据附件二所列的欧盟统一立法，将该产品投放市场或投入使用；
2. 除第1款所指的高风险人工智能系统外，附件三所指的人工智能系统也应被视为高风险系统。
2a. 根据第2款的克减规定，如果人工智能系统对自然人的健康、安全或基本权利不构成重大损害风险，包括不对决策结果产生重大影响，则不应被视为高风险系统。如果符合以下一项或多项标准，则属于这种情况：
(a) 人工智能系统旨在执行范围狭窄的程序性任务；
(b) 人工智能系统旨在改进先前完成的人类活动的结果；
(c) 人工智能系统的目的是检测决策模式或偏离先前决策模式的情况，而不是在未经适当人工审查的情况下取代或影响先前完成的人工评估；或
(d) 该人工智能系统的目的是为附件三所列的用例进行相关评估做准备。
尽管存在本款第一项的规定，但如果人工智能系统对自然人进行画像，该系统应始终被视为高风险系统。
2b. 认为附件三所述人工智能系统不属于高风险系统的提供者应在该系统投放市场或投入使用之前将其评估结果记录在案。该提供者应履行第51条第1a款规定的登记义务。应国家主管机关的要求，提供者应提供评估文件。
2c. 委员会应在征求欧洲人工智能委员会的意见后，在本条例生效后18个月内，根据第82b条的规定，提供具体实施本条款的指南，并附上人工智能系统高风险和非高风险使用案例的综合实例清单。
2d. 委员会有权根据第73条通过授权法案，修改第2a款第1项第a至d点规定的标准。

只有在有具体和可靠的证据表明存在属于附件三范围的人工智能系统，但不会对健康、安全和基本权利造成重大危害的情况下，欧盟委员会才可以通过授权法案，在第2a款第1项第a至d点规定的标准之外增加新的标准，或修改这些标准。
委员会应通过授权法案，删除第2a款第1项规定的任何标准，只要有具体和可靠的证据表明有必要这样做，以保持欧盟对健康、安全和基本权利的保护水平。对第2a款第1项第a至d点规定的标准的任何修改，不得降低欧盟在保护健康、安全和基本权利方面的整体水平。在通过授权法案时，欧盟委员会应确保与根据第7条第1款通过的授权法案保持一致，并应考虑到市场和技术的发展。

第7条
对附件三的修正

1. 委员会有权根据第73条通过授权法案，对附件三进行修正，增加或修改符合以下两个条件的高风险人工智能系统的用例：
(a) 拟在附件三第1至第8点所列的任何领域使用人工智能系统；
(b) 人工智能系统有可能对健康和安全造成危害，或对基本权利造成不利影响，而且这种风险等同于或大于附件三已提及的高风险人工智能系统所造成的危害或不利影响。
2. 为第1款之目的，在评估一个人工智能系统对健康和安全造成危害的风险或对基本权利造成不利影响的风险是否等同于或大于附件三已提及的高风险人工智能系统造成危害的风险时，委员会应考虑以下标准：
(a) 人工智能系统的预期目的；
(b) 已使用或可能使用人工智能系统的程度；
(ba) 人工智能系统处理和使用的数据的性质和数量，特别是是否处理特殊类别的个人数据；
(bb) 人工智能系统自主性的程度，以及人类推翻可能导致潜在伤害的决定或建议的可能性；
(c) 人工智能系统的使用在多大程度上已经对健康和安全造成了损害，对基本权利产生了不利的影响，或在多大程度上引起了人们对这种损害或不利影响的可能性的严重关注，例如，提交给国家主管机关的报告或有据可查的指控，或酌情提交的其他报告所表明的情况。
(d) 这种损害或不利影响的潜在程度，特别是其严重程度及其影响多数人或不成比例地影响特定群体的能力；
(e) 可能受到伤害或不利影响的人在多大程度上依赖人工智能系统产生的结果，特别是由于实际或法律原因而无法合理地选择不接受该结果；
(f) 权力不平衡的程度，或可能受到伤害或不利影响的人相对于人工智能系统用户而言处于弱势地位的程度，特别是由于地位、权力、知识、经济或社会环境或年龄等原因；
(g) 人工智能系统产生的结果在多大程度上易于纠正或逆转，同时考虑到现有的纠正或逆转的技术解决方案，其中对健康、安全、基本权利有不利影响的结果不应被视为易于纠正或逆转；
(gb) 部署人工智能系统对个人、群体或整个社会的好处的程度和可能性，包括对产品安全的可能改进；

(h) 现有欧盟立法在多大程度上规定了：
(i) 针对人工智能系统带来的风险采取有效的救济措施，但不包括损害赔偿要求；
(ii) 采取有效措施预防或最大限度地降低这些风险。
2a. 欧盟委员会有权根据第73条通过授权法案，修改附件三的清单，删除同时满足以下两个条件的高风险人工智能系统：
(a) 考虑到第2款所列标准，有关的高风险人工智能系统不再对基本权利、健康或 安全构成任何重大风险；
(b) 删除不会降低欧盟法律对健康、安全和基本权利的总体保护水平。

第二章
高风险人工智能系统的要求

第8条
符合要求

1. 高风险人工智能系统应符合本章规定的要求，同时考虑到其预期目的以及人工智能和人工智能相关技术的公认技术水平。在确保遵守这些要求时，应考虑到第9条所述的风险管理系统。
2a. 如果产品包含人工智能系统，而本条例的要求以及附件二A部分所列欧盟统一立法的要求适用于该产品，则提供者应负责确保其产品完全符合欧盟统一立法要求的所有适用要求。
在确保第1款中提及的高风险人工智能系统符合本编第二章中规定的要求时，为了确保一致性、避免重复和尽量减少额外的负担，提供者应可选择酌情将其提供的有关其产品的必要检测和报告过程、信息和文件纳入附件二A部分所列欧盟统一立法要求的现有文件和程序中。

第9条
风险管理系统

1. 应建立、实施、记录和维护与高风险人工智能系统有关的风险管理系统。
2. 风险管理系统应被理解为在高风险人工智能系统的整个生命周期内规划和运行的一个持续迭代过程，需要定期进行系统审查和更新. 其应包括以下步骤
(a) 识别和分析高风险人工智能系统在按照其预期用途使用时可能对健康、安全或基本权利造成的已知和可合理预见的风险；
(b) 估计和评估高风险人工智能系统在按照其预期目的和在可合理预见的滥用条件下使用时可能出现的风险；
(c) 根据对从第61条提及的后市场监测系统中收集到的数据的分析，评估其他可能出现的风险；
(d) 根据以下各段的规定，采取适当的、有针对性的风险管理措施，以应对本段第a点所确定的风险。
2a. 本段所指的风险只涉及那些通过开发或设计高风险人工智能系统或提供充分的技术信息可以合理减轻或消除的风险。
3. 第2款第d点提及的风险管理措施应适当考虑第二章规定的各项要求的综合应

用所产生的影响和可能的相互作用，以便更有效地将风险降至最低，同时在执行措施以满足这些要求时实现适当的平衡。
4. 第2款第d点所述的风险管理措施应使与每种危险相关的残余风险以及高风险人工智能系统的总体残余风险被判定为可以接受。
在确定最合适的风险管理措施时，应确保以下几点：
(a) 通过充分设计和开发高风险人工智能系统，在技术上可行的情况下，消除或减少根据第2款确定和评估的风险；
(b) 酌情实施适当的缓解和控制措施，以应对无法消除的风险；
(c) 根据本条第2款第b点所述第13条的规定提供必要的信息，并酌情对部署者进行培训。
为了消除或减少与使用高风险人工智能系统有关的风险，应适当考虑部署者的技术知识、经验、教育、预期培训以及意图使用该系统的假定环境。
5. 应测试高风险人工智能系统，以确定最适当和最有针对性的风险管理措施。测试应确保高风险人工智能系统能始终如一地达到预期目的，并符合本章规定的要求。
6. 测试程序可包括根据第54a条在真实世界条件下进行的测试。
7. 对高风险人工智能系统的测试应酌情在整个开发过程的任何时候进行，无论如何应在投放市场或投入使用之前进行。应根据事先确定的指标和概率阈值进行测试，这些指标和阈值应适合高风险人工智能系统的预期目的。
8. 在实施第1至第6款所述风险管理系统时，提供者应考虑高风险人工智能系统的预期目的是否可能对18岁以下的个人产生不利影响，并酌情对其他弱势群体产生不利影响。
9. 对于高风险人工智能系统的提供者而言，如果其内部风险管理流程须符合相关部门联盟法律的要求，则第1至第8款所述方面可作为根据该法律制定的风险管理程序的一部分或与之相结合。

第10条
数据和数据治理

1. 使用数据训练模型技术的高风险人工智能系统，应在使用符合第2至第5款所述质量标准的训练、验证和测试数据集的基础上开发。
2. 训练、验证和测试数据集应遵守适合人工智能系统预期目的的适当的数据治理和管理实践。这些实践应特别涉及
(a) 相关的设计选择；
(aa) 数据收集过程和数据来源，如果是个人数据，还应说明收集数据的初始目的；
(c) 相关的数据准备处理操作，如注释、标记、清理、更新、丰富和汇总；
(d) 提出假设，特别是关于数据应衡量和代表的信息的假设；
(e) 评估所需数据集的可用性、数量和适用性；
(f) 审查可能存在的偏差，这些偏差可能影响人员的健康和安全，对基本权利产生负面影响，或导致欧盟法律所禁止的歧视，特别是在数据输出影响未来的运营投入的情况下；
(fa) 采取适当措施，发现、防止和减少根据第f点确定的可能的偏见；
(g) 确定妨碍遵守本条例的相关的数据差距或缺陷，以及如何解决这些差距和

缺陷。
3.训练、验证和测试数据集应具有相关性和充分的代表性，并在尽最大可能的范围内没有错误，并且从预期目的来看是完整的。数据集应具有适当的统计特性，包括在适用的情况下，与意图使用高风险人工智能系统的个人或群体有关的统计特性。数据集的这些特性可以在单个数据集或数据集组合的层面上得到满足。
4.数据集应在预期目的要求的范围内，考虑到高风险人工智能系统预期使用的具体地理、场景、行为或功能环境所特有的特征或要素。
5.在确保根据第二段第f点和fa点对高风险人工智能系统进行偏差检测和纠正的严格必要范围内，此类系统的提供者可例外处理2016/679号条例第9条第1款、2016/680号指令第10条和2018/1725号条例第10条第1款中提及的特殊类别个人数据，但须适当保障自然人的基本权利和自由。除2016/679号条例、2016/680号指令和2018/1725号条例的规定外，以下所有条件均应适用，以便开展此类处理：
(a) 通过处理其他数据，包括合成数据或匿名数据，无法有效实现偏差检测和纠正；
(b) 为本款目的而处理的特殊类别个人数据在个人数据的重复使用方面受到技术限制，并采取最先进的安全和隐私保护措施，包括假名化；
(c) 为本段目的而处理的特殊类别个人数据须遵守相关措施，以确保所处理的个人数据安全、受保护、具备适当的保障措施，包括严格的访问记录和控制，以避免滥用， 并确保只有经授权的人才能访问这些个人数据，并承担适当的保密义务；
(d) 不得将为本段之目的处理的特殊类别个人数据传输、转让或以其他方式提供给其他方；
(e) 一旦偏差得到纠正或个人数据的保存期结束，以先到期者为准，即删除为本款目的而处理的特殊类别个人数据；
(f) 根据2016/679号条例、2016/680 号指令和2018/1725号条例进行的处理活动记录，包括处理特殊类别个人数据对于检测和纠正偏见是严格必要的，且这一目标无法通过处理其他数据来实现的理由。
6.对于不使用涉及模型训练技术的高风险人工智能系统的开发，第2至第5款仅适用于测试数据集。

第11条
技术文件

1.高风险人工智能系统的技术文件应在该系统投放市场或投入使用之前编制，并应不断更新。技术文件的编制应能证明高风险人工智能系统符合本章规定的要求，并以清晰和全面的形式向国家主管机关和通知机关提供必要的信息，以评估人工智能系统是否符合这些要求。它至少应包含附件四所列的要件。小微型企业，包括初创企业，可以简化方式提供附件四中规定的技术文件要素。为此，委员会应针对小型和微型企业的需要制定简化的技术文件格式。如果小微型企业，包括初创企业，选择以简化方式提供附件四所要求的信息，则应使用本款中提到的表格。通知机关应接受该表格用于合格性评估。
2.如果附件二A节所列法律适用于某一产品的高风险人工智能系统投放市场或投

入使 用，则应编制一份单一的技术文件，其中包含第1款规定的所有信息以及这些法律所要求的信息。
3. 委员会有权根据第73条的规定通过授权法案，对附件四进行必要的修改，以确保在技术进步的情况下，技术文件能提供评估系统是否符合本章要求的所有必要信息。

第12条
记录留存

1. 高风险人工智能系统应在技术上允许自动记录系统生命周期内的事件，即日志。
2. 为了确保人工智能系统功能的可追溯程度与系统的预期目的相适应，日志记录功能应能够记录与以下方面相关的事件：
2a. (i) 确定可能导致人工智能系统产生第65条第1款意义上的风险或进行实质性修改的情况；
(ii) 促进第61条所述的后市场监测；以及
(iii) 监督第29条第4款所述高风险人工智能系统的运行。
4. 对于附件三第1款第a节所述的高风险人工智能系统，日志记录能力至少应具备以下功能
(a) 记录每次使用系统的时间，每次使用的开始日期和时间以及结束日期和时间；
(b) 系统对输入数据进行核对的参考数据库；
(c) 搜索结果匹配的输入数据；
(d) 第14条第5款所述参与核查结果的自然人的身份。

第13条
透明度和向部署者提供信息

1. 高风险人工智能系统的设计和开发应确保其操作具有足够的透明度，使部署者能够解释系统的输出并加以适当使用。应确保适当类型和程度的透明度，以遵守本编第三章规定的提供者和部署者的相关义务。
2. 高风险人工智能系统应附有适当的数字格式或其他形式的使用说明，其中包括简明、完整、正确和清晰的信息，这些信息应与用户相关、便于用户使用和理解。
3. 使用说明应至少包含以下信息：
(a) 提供者及其授权代表，如适用，的身份和联系方式；
(b) 高风险人工智能系统的特点、能力和性能限制，包括
(i) 其预期目的；
(ii) 高风险人工智能系统经过测试和验证并可预期的准确性水平，包括第15条所指的度量、稳健性和网络安全，以及可能对预期的准确性水平、稳健性和网络安全产生影响的任何已知和可预见的情况；
(iii) 任何已知的或可预见的、与高风险人工智能系统按其预期目的使用或在可 合理预见的滥用条件下使用有关的、可能导致第9条第2款所述的健康和安全或基本权利风险的情况；

(iiia) 在适用情况下，人工智能系统提供与解释其产出相关的信息的技术能力和特点。
(iv) 在适当情况下，该系统对意图使用该系统的特定个人或群体的性能；
(v) 在适当情况下，考虑到人工智能系统的预期目的，提供输入数据的规格，或所使用的训练、验证和测试数据集方面的任何其他相关信息。
(va) 在适用的情况下，提供信息，使得部署者能够解释系统的输出结果并加以适当使用。
(c) 对高风险人工智能系统及其性能所做的修改，如果有的话，这些修改是由提供者在初次合格性评估时预先确定的；
(d) 第14条所述的人工监督措施，包括为便于部署者解释人工智能系统的输出结果而采取的技术措施；
(e) 所需的计算和硬件资源，高风险人工智能系统的预期寿命，以及任何必要的维护和保养措施，包括其频率，以确保该人工智能系统的正常运行，包括软件更新；
(ea) 在相关情况下，说明人工智能系统所包含的机制，使用户能够根据第12条的规定适当地收集、储存和解释日志。

第14条
人类监督

1. 高风险人工智能系统的设计和开发方式，包括适当的人机交互接口工具，应能在人工智能系统使用期间由自然人进行有效监督。
2. 人的监督应旨在防止或最大限度地减少高风险人工智能系统在按其预期目的使用时或在可合理预见的滥用条件下使用时可能对健康、安全或基本权利造成的风险，特别是在尽管适用了本章规定的其它要求但这种风险依然存在的情况下。
3. 监督措施应与人工智能系统的风险、自主程度和使用环境成比例，并应通过以下一种或所有类型的措施加以确保：
(a) 提供者在高风险人工智能系统投放市场或投入使用之前，在技术上可行的情况下，在该系统中确定和建立的措施；
(b) 提供者在将高风险人工智能系统投放市场或投入使用之前确定的、适合由用户实施的措施。
4. 为执行第1至第3款，向用户提供高风险人工智能系统时，应酌情并根据具体情况，使被指派进行人工监督的自然人能够使用该系统：
(a) 适当了解高风险人工智能系统的相关能力和局限性，并能适当监测其运行情况，以及发现和处理异常情况、功能失调和意外表现；
(b) 始终意识到自动依赖或过度依赖高风险人工智能系统产生的输出结果（“自动化偏差”）的可能趋势，特别是对于用于为自然人决策提供信息或建议的高风险人工智能系统；
(c) 正确解释高风险人工智能系统的输出结果，同时考虑现有的解释工具和方法；
(d) 在任何特定情况下决定不使用高风险人工智能系统，或以其他方式忽略、推翻或逆转高风险人工智能系统的输出；
(e) 通过“停止”按钮或类似程序，干预高风险人工智能系统的运行或中断系

统，使系统停 止在安全状态。
5. 对于附件三第1a点所述的高风险人工智能系统，第3款所述的措施应确保，除此之外，部署者不得根据该系统产生的识别结果采取任何行动或做出任何决定，除非至少有两个具有必要的能力、培训和授权的自然人分别加以核实和确认。
在欧盟或国家法律认为适用这一要求不成比例的情况下，至少由两个自然人分别进行核查的要求不应适用于用于执法、移民、边境管制或庇护目的的高风险人工智能系统。

第15条
准确性、稳健性和网络安全

1. 在设计和开发高风险人工智能系统时，应使其达到适当的准确性、稳健性和网络安全水平，并在其整个生命周期内始终在这些方面保持一致。
1a. 为解决如何衡量本条第1款规定的适当准确性和稳健性水平以及任何其他相关性能指标的技术问题，委员会应与利益相关方和组织（如计量和基准制定机构）合作，酌情鼓励制定基准和衡量方法。
2. 高风险人工智能系统的准确度等级和相关准确度指标应在随附的使用说明中公布。
3. 高风险人工智能系统应尽可能避免系统内部或系统运行环境中可能出现的错误、故障或不一致，特别是由于系统与自然人或其他系统的互动而造成的错误、故障或不一致。在这方面应采取技术和组织措施。
高风险人工智能系统的稳健性可通过技术冗余解决方案来实现，其中可能包括备份或故障安全计划。
高风险人工智能系统在投放市场或投入使用后仍在继续学习，其开发方式应尽可能消除或减少可能有偏差的输出影响未来操作输入的风险（“反馈回路”），并采取适当的缓解措施。
4. 高风险人工智能系统应具备韧性，以防未经授权的第三方试图利用系统漏洞改变其使用、输出或性能。
旨在确保高风险人工智能系统网络安全的技术解决方案应与相关情况和风险相适应。
处理人工智能特定漏洞的技术解决方案应酌情包括以下措施：预防、检测、应对、解决和控制试图篡改训练数据集（“数据投毒”）或篡改用于训练的预训练组件（“模型投毒”）的攻击、旨在导致模型出错的输入（“对抗性示例”或“模型规避”）、保密性攻击或者模型的缺陷。

第3章
高风险人工智能系统的提供者和部署者以及其他各方的义务

第16条
高风险人工智能系统提供者的义务

高风险人工智能系统的提供者应
(a) 确保其高风险人工智能系统符合本编第二章的要求；

(aa) 在高风险人工智能系统上标明其名称、登记商号或登记商标、联系地址，如无法标明，则在包装或随附文件上标明；
(b) 具有符合第17条规定的质量管理体系；
(c) 保存第18条提及的文件；
(d) 在其控制下保存第20条所述高风险人工智能系统自动生成的日志；
(e) 确保高风险人工智能系统在投放市场或投入使用之前经过第43条所述的相关合格性评估程序；
(ea) 根据第48条的规定，起草欧盟合格性声明；
(eb) 根据第49条的规定，在高风险人工智能系统上加贴CE标志，以表明其符合本条例的规定；
(f) 遵守第51条第1款所述的登记义务；
(g) 采取必要的纠正措施，并提供第21条所要求的信息；
(j) 应国家主管机关的合理要求，证明高风险人工智能系统符合本编第二章的要求；
(ja) 确保高风险人工智能系统符合无障碍要求，符合关于产品和服务无障碍要求的2019/882号指令和关于公共部门机构网站和移动应用程序无障碍要求的2016/2102号指令。

第17条
质量管理系统

1. 高风险人工智能系统的提供者应建立质量管理体系，确保遵守本条例。该系统应以书面政策、程序和指令的形式系统有序地加以记录，并至少应包括以下方面：
(a) 合规策略，包括遵守合格性评估程序和管理修改高风险人工智能系统的程序；
(b) 用于高风险人工智能系统的设计、设计控制和设计验证的技术、程序和系统行动；
(c) 用于高风险人工智能系统的开发、质量控制和质量保证的技术、程序和系统行动；
(d) 在开发高风险人工智能系统之前、期间和之后要进行的检查、测试和验证程序，以及进行这些程序的频率；
(e) 应采用的技术规格，包括标准，如果没有完全采用相关的统一标准，或没有涵盖本编第二章所列的所有相关要求，应采用何种手段确保高风险人工智能系统符合这些要求；
(f) 数据管理的系统和程序，包括数据获取、数据收集、数据分析、数据标示、数据存储、数据过滤、数据挖掘、数据汇总、数据保留，以及在高风险人工智能系统投放市场或投入使用前和为投放市场或投入使用而进行的与数据有关的任何其他操作；
(g) 第9条提及的风险管理系统；
(h) 根据第61条的规定，建立、实施和维护市场后监测系统；
(i) 根据第62条报告严重事件的相关程序；
(j) 处理与国家主管机关、其他相关机构（包括提供或支持数据访问的机构）、通知机关、其他运营商、客户或其他相关方的沟通；

(k) 所有相关文件和信息的记录保存系统和程序；
(l) 资源管理，包括与供应安全有关的措施；
(m) 问责框架，规定管理层和其他工作人员在本段所列各方面的责任。
2. 第1款所述各方面的实施应与提供者组织的规模成比例。在任何情况下，提供者都应尊重为确保其人工智能系统符合本条例所要求的严格程度和保护水平。
2a. 对于高风险人工智能系统的提供者来说，如果根据相关的欧盟部门法必须履行质量管理系统方面的义务，那么第1款描述的方面可以是该法律规定的质量管理系统的一部分。
3. 对于须遵守欧盟金融服务立法对其内部治理、安排或流程要求的金融机构，除第1款第g、h和i点外，建立质量管理体系的义务应视为通过遵守相关欧盟金融服务立法的内部治理安排或流程规则来履行。在这种情况下，应考虑本条例第40条提及的任何统一标准。

第18条
文件保存

1. 在人工智能系统投放市场或投入使用后的10年内，提供者应随时向国家主管机关报告：
(a) 第11条提及的技术文件；
(b) 第17条提及的有关质量管理体系的文件；
(c) 在适用的情况下，与通知机关批准的变更有关的文件；
(d) 通知机关发布的决定和其他文件，如适用；
(e) 第 48 条所述的欧盟合格性声明。
1a. 各成员国应确定在第1款所述期限内，国家主管机关仍可处置该段所述文件的条件，如果在其领土上设立的提供者或其授权代表在该期限结束前破产或停止活动。
2. 根据欧盟金融服务立法，作为金融机构的提供者，其内部治理、安排或流程须符合相关要求，因此应将技术文件作为根据相关欧盟金融服务立法保存的文件的一部分进行保存。

第20条
自动生成日志

1. 高风险人工智能系统的提供者应保存第12条第1款所述由其高风险人工智能系统自动生成的日志，只要这些日志在其控制范围内。在不影响适用的欧盟或国家法律的情况下，日志的保存期限应与高风险人工智能系统的预期目的相适应，至少为6个月，除非适用的欧盟或国家法律，特别是欧盟关于保护个人数据的法律另有规定。
2. 根据欧盟金融服务立法，金融机构的内部管理、安排或流程必须符合相关要求，提供者应保存其高风险人工智能系统自动生成的日志，作为根据相关金融服务立法保存的文件的一部分。

第21条
纠正行动和提供信息的义务

高风险人工智能系统的提供者如认为或有理由认为其投放市场或投入使用的高风险人工智能系统不符合本条例的规定，应立即采取必要的纠正措施，使该系统符合规定，酌情予以撤回、禁用或召回。他们应通知有关高风险人工智能系统的分销者，并酌情通知部署者、授权代表和进口者。
如果高风险人工智能系统存在第65条第1款意义上的风险，且提供者意识到该风险，则应立即与报告风险的部署者，如适用，合作调查原因，并通知其提供高风险人工智能系统所在成员国的市场监督管理机关，以及根据第44条为高风险人工智能系统颁发认证的通知机关，如适用，特别是不合规的性质和采取的任何相关纠正措施。

第23条
与主管机关的合作

高风险人工智能系统的提供者应在主管机关提出合理要求时，向该机关提供证明高风险人工智能系统符合本编第2章规定的要求所需的所有信息和文件，其语言应为有关成员国确定的联盟官方语言，易于该机关理解。
1a 在国家主管机关提出合理要求后，提供者还应酌情允许提出要求的国家主管机关查阅高风险人工智能系统自动生成的第12条第1款所述的日志，只要这些日志在其控制之下。
(1b) 国家主管机关根据本条规定获得的任何信息应按照第70条规定的保密义务处理。

第25条
授权代表

1. 在联盟外设立的提供者在联盟市场上提供其系统之前，应通过书面授权，指定一名在联盟内设立的授权代表。
1b. 提供者应使其授权代表能够执行本条例规定的任务。
2. 授权代表应执行提供者授权中规定的任务。授权代表应根据请求，以国家主管机关确定的联盟机构官方语言之一，向市场监督管理机关提供一份授权副本。就本条例而言，授权应授权受权代表执行以下任务：
(-a) 核实欧盟合格性声明和技术文件是否已经拟定，以及提供者是否已经执行了适当的合格性评估程序；
(a) 在高风险人工智能系统投放市场或投入使用后10年内，向国家主管机关和第63条第7款所指的国家机关提供指定授权代表的提供者的详细联系信息、欧盟合格性声明副本、技术文件以及（如适用）通知机关签发的认证；
(b) 在国家主管机关提出合理要求时，向其提供证明高风险人工智能系统符合本编第 2 章规定的要求所需的所有信息和文件，包括根据第b点保存的信息和文件，包括查阅第12条第1款所述的由高风险人工智能系统自动生成的日志，只要这些日志在提供者的控制之下；
(c) 应主管机关的合理要求，就后者对高风险人工智能系统采取的任何行动与主管机关合作，特别是减少和降低高风险人工智能系统带来的风险；
(ca) 在适用的情况下，遵守第51条第1款所述的登记义务，或者，如果登记由

提供者自己进行，则确保附件八第3点所述的信息正确无误。
2a 授权书应授权七授权代表，在与确保遵守本条例有关的所有问题上，除提供者外，或代替提供者，接受主管机关的问询。
2b.如果授权代表认为或有理由认为提供者的行为违反了本条例规定的义务，则应终止授权。在这种情况下，授权代表还应立即向其所在成员国的国家监管机关，并在适用情况下向相关通知机关通报任务终止情况及其原因。

第26条
进口者的义务

1.在将高风险人工智能系统投放市场之前，该系统的进口者应确保该系统符合本条例的规定，方法是核实：
(a) 该人工智能系统的提供者已执行了第43条所述的相关合格性评估程序；
(b) 提供者已根据条款和附件四编制了技术文件；
(c) 系统带有所需的CE合格性标志，并附有欧盟合格性声明和使用说明；
(ca) 提供者已根据第25条第1款的规定任命了授权代表。
2.如果进口者有充分理由认为高风险人工智能系统不符合本条例的规定，或者系统是伪造的，或者附有伪造的文件，在该人工智能系统符合规定之前，进口者不得将该系统投放市场。如果高风险人工智能系统具有第65条第1款所指的风险，进口者应将此情况通知人工智能系统的提供者、授权代表和市场监督管理机关。
3.进口者应在高风险人工智能系统及其包装或随附文件，如适用，上注明其名称、登记商号或登记商标以及联系地址。
4.进口者应确保，当高风险人工智能系统由其负责时，在适用的情况下，储存或运输条件不会危及该系统符合本编第2章规定的要求。
4a.进口者应在人工智能系统投放市场或投入使用后的10年内，保存一份由通知机关签发的认证副本（如适用）、使用说明和欧盟合格性声明。
5.进口者应在国家主管机关提出合理要求时，以其易于理解的语言向其提供所有必要的资料和文件，包括按照第4a款保存的资料和文件，以证明高风险人工智能系统符合本编第2章的要求。为此，它们还应确保向这些机关提供技术文件。
5a.进口者应就国家主管机关采取的任何行动与国家主管机关合作，特别是为减少和降低高风险人工智能系统带来的风险。

第27条
分销者的义务

1.在市场上销售高风险人工智能系统之前，分销者应核实高风险人工智能系统是否带有所需的CE合格性标识，是否附有欧盟合格性声明和使用说明的副本，以及系统的提供者和进口者，如适用，是否分别遵守了第16条第b点和第26条第3款规定的义务。
2.如果分销者根据其掌握的信息认为或有理由认为高风险人工智能系统不符合本编第2章规定的要求，在该系统符合这些要求之前，分销者不得在市场上销售该高风险人工智能系统。此外，如果该系统存在第65条第1款所指的风险，分销

者应酌情将此情况通知该系统的提供者或进口者。
3.分销者应确保，当高风险人工智能系统由其负责时，在适用的情况下，储存或运输条件不会危及该系统符合本编第2章的要求。
4. 分销者如根据其掌握的信息认为或有理由认为其在市场上提供的高风险人工智能系统不符合本编第2章规定的要求，则应采取必要的纠正措施，使该系统符合这些要求，撤回或召回该系统，或应确保提供者、进口者或任何有关经营者酌情采取这些纠正措施。如果高风险人工智能系统存在第65条第1款所指的风险，分销者应立即将此情况通知该系统的提供者或进口者以及其提供产品的成员国的国家主管机关，特别是提供不符合要求的详细情况和所采取的纠正措施。
5.在国家主管机关提出合理要求后，高风险人工智能系统的分配者应向该主管机关提供第1至第4款所述的有关其活动的所有必要信息和文件，以证明高风险系统符合本编第2章规定的要求。
5a.分销者应就国家主管机关对其作为分销者的人工智能系统采取的任何行动与国家主管机关合作，特别是为了减少或降低高风险人工智能系统造成的风险。

第28条
人工智能价值链上的责任

1. 为本条例之目的，任何分销者、进口者、部署者或其他第三方均应视为高风险人工智能系统的提供者，在下列任何一种情况下，均应承担第16条规定的提供者义务：
(a) 在已投放市场或投入使用的高风险人工智能系统上冠以自己的名称或商标，但不妨碍合同中关于以其他方式分配义务的规定；
(b) 对已投放市场或已投入使用的高风险人工智能系统进行实质性修改，但改造方式仍符合第6条规定的高风险人工智能系统；
(ba) 其修改了一个人工智能系统，包括通用人工智能系统，的预定用途，而该人工智能系统尚未被归类为高风险，并已投放市场或投入使用，从而使该人工智能系统成为第6条所指的高风险人工智能系统。
2.如果出现第1款第a至ba项所述情况，最初将人工智能系统投放市场或投入使用的提供者将不再被视为本条例所指的特定人工智能系统的提供者。该在先提供者应密切合作，提供必要的信息，并提供合理预期的技术准入和其他协助，以履行本条例规定的义务，特别是关于遵守高风险人工智能系统合格性评估的义务。
本款不适用于在先提供者明确排除将其系统改为高风险系统并因此排除移交文件义务的情况。
2a.对于作为附件二A节所列法律行为适用产品的安全组件的高风险人工智能系统，这些产品的制造商应被视为高风险人工智能系统的提供者，并应在以下任一情况下履行第16条规定的义务：
(i) 高风险人工智能系统以产品制造商的名称或商标与产品一起投放市场；
(ii) 产品投放市场后，高风险人工智能系统以产品制造商的名义或商标投入使用。
2b.高风险人工智能系统的提供者和提供人工智能系统、工具、服务、组件或高风险人工智能系统中使用或集成的程序的第三方，应通过书面协议，根据公认

的技术水平，具体说明必要的信息、能力、技术访问和其他援助，以使高风险人工智能系统的提供者能够完全遵守本条例规定的义务。该义务不适用于在免费开放许可下向公众提供工具、服务、流程或人工智能组件，通用人工智能模型除外，的第三方。
人工智能办公室可制定和推荐高风险人工智能系统提供者与提供高风险人工智能系统使用或集成的工具、服务、组件或流程的第三方之间的自愿性示范合同条款。
在制定自愿性示范合同条款时，人工智能办公室应考虑到适用于特定部门或商业用例的可能的合同要求。合同条款范本应以易于使用的电子格式公布并免费提供。
2b. 第2款和第2a款不影响根据欧盟法律和国家法律尊重和保护知识产权、商业机密信息或商业秘密的必要性。

第29条
高风险人工智能系统部署者的义务

1. 高风险人工智能系统的部署者应采取适当的技术和组织措施，确保按照本条第2款和第5款的规定，根据系统所附的使用说明使用这些系统。
1a. 部署者应指派具备必要能力、培训和权力以及必要支持的自然人进行人工监督。
1a. 在部署者对高风险人工智能系统行使控制权的情况下，他们应确保被指派确保对高风险人工智能系统进行人为监督的自然人具备必要的能力、培训和权力以及必要的支持。
2. 第1款和第1a款中的义务不影响欧盟或国家法律规定的其他部署者义务，也不影响部署者为实施提供者所述的人员监督措施而自行安排资源和活动的自由裁量权。
3. 在不影响第1款和第1a款的情况下，如果部署者对输入数据行使控制权，则应确保输入数据与高风险人工智能系统的预期目的相关并具有充分代表性。
4. 部署者应根据使用说明监测高风险人工智能系统的运行情况，并在必要时根据第61条通知提供者。当其有理由认为按照使用说明使用可能导致人工智能系统出现第65条第1款所指的风险时，其应立即通知提供者或经销商和有关市场监督管理机关，并暂停使用该系统。如果部署者无法联系到提供者，则应比照适用第62条。这项义务不包括作为执法机关的人工智能系统用户的敏感操作数据。
对于根据欧盟金融服务立法须遵守内部治理、安排或流程要求的金融机构部署者而言，遵守相关金融服务立法规定的内部治理安排、流程和机制规则，即视为履行了本款第1段规定的监控义务。
5. 高风险人工智能系统的部署者应留存该高风险人工智能系统自动生成的日志，留存期限应与高风险人工智能系统的预期目的相符，至少6个月，除非适用的欧盟或国家法律，特别是欧盟关于保护个人数据的法律另有规定。
如果部署者是金融机构，须遵守联盟金融服务立法对其内部治理、安排或流程的要求，则应保存日志，作为根据相关联盟金融服务立法保存的文件的一部分。
(a) 在工作场所投入或使用高风险人工智能系统之前，作为雇主的部署者应告

知工人代表和受影响的工人，他们将受到该系统的影响。在适用的情况下，应根据联盟和国家关于工人及其代表信息的法律和实践中规定的规则和程序提供这些信息。
(b) 作为公共机关或欧盟机构、机关、办公室和机构的高风险人工智能系统的部署者应遵守第51条所述的登记义务。当他们发现他们意图使用的系统尚未在第60条提及的欧盟数据库中登记时，他们不得使用该系统，并应通知提供者或经销商。
(c) 作为公共机关的高风险人工智能系统部署者，包括第51条第1a款第b项提及的联盟机构、机关、办公室和机构，应遵守第51条提及的登记义务。
6. 在适用的情况下，高风险人工智能系统的部署者应使用第13条提供的信息，以履行其根据以下规定进行数据保护影响评估的义务，2016/679号条例第35条或2016/680号指令第27条。
6a. 在不影响2016/680号指令的情况下，在对被判定或涉嫌犯有刑事罪的人进行定向搜查的调查框架内，用于事后远程生物特征识别的人工智能系统的部署者应在使用该系统之前，或在不无故拖延且不迟于48小时的情况下，请求司法机关或其决定具有约束力并可接受司法审查的行政机关授权使用该系统，除非该系统是用于根据与犯罪直接相关的客观和可核实的事实初步识别潜在嫌疑人。每次使用应仅限于调查具体刑事犯罪所严格需要的范围。
如果本款第一分段规定的授权请求被拒绝，则应立即停止使用与该授权请求相关联的事后远程生物识别系统，并删除与使用该系统相关联的个人数据。
在任何情况下，这种用于事后远程生物识别的人工智能系统都不得在与刑事犯罪、刑事诉讼、真实存在的或真实可预见的刑事犯罪威胁或寻找特定失踪人员没有任何联系的情况下，普遍地用于执法目的。
应确保执法机关不得仅根据这些远程生物识别系统的输出结果做出对个人产生不利法律影响的决定。
本段不影响2016/680号指令第10条和《通用数据保护条例》第9条关于生物识别数据处理的规定。
无论目的或部署者如何，这些系统的每次使用都应记录在相关的警方档案中，并应要求提供给相关市场监督管理机关和国家数据保护机构，但不包括与执法有关的敏感业务数据的披露。本分段不应妨碍2016/680号指令赋予监管机关的权力。
此外，部署者应向有关市场监督管理机关和国家数据保护机构提交年度报告，说明事后远程生物识别系统的使用情况，但不包括与执法有关的敏感业务数据的披露。报告可以汇总，以涵盖一次行动中的若干部署情况。
成员国可根据欧盟法律，对使用事后远程生物识别系统制定限制性更强的法律。
6b. 在不影响第52条规定的情况下，附件三所述高风险人工智能系统的部署者在做出或协助做出与自然人有关的决定时，应告知自然人其须使用高风险人工智能系统。对于用于执法目的的高风险人工智能系统，应适用2016/680号指令第13条。
6c. 部署者应与相关国家主管机关合作，采取与高风险系统有关的任何行动，以执行本条例。

第29a条

高风险人工智能系统的基本权利影响评估

1.在部署第6条第2款定义的高风险人工智能系统投入使用之前，除意图用于附件三第2点所列领域的人工智能系统外，受公法管辖的机构或提供公共服务的私人运营商以及部署附件三第5项第b和d点所述高风险系统的运营商应评估使用该系统可能对基本权利产生的影响。为此，部署者应进行以下评估：
a）说明部署者按照预期目的使用高风险人工智能系统的过程；
b）说明每个高风险人工智能系统的使用期限和频率
c）在特定情况下，可能受其使用影响的自然人和群体的类别；
d）考虑到提供者根据第13条提供的信息，根据第c点确定的人员类别或群体可能受到的具体的损害风险；
e）根据使用说明，说明人的监督措施的执行情况；
f）出现这些风险时应采取的措施，包括内部管理和投诉机制的安排。
2.第1款规定的义务适用于高风险人工智能系统的首次使用。在类似情况下，部署者可依赖以前进行的基本权利影响评估或提供者进行的现有影响评估。如果在使用高风险人工智能系统期间，部署者认为第1款所列的任何因素发生变化或不再是最新的，部署者将采取必要步骤更新信息。
3.一旦进行了影响评估，部署者应将评估结果通知市场监督管理机关，并提交第5款所述的填写模板作为通知的一部分。在第47条第1款所述的情况下，部署者可免除这些义务。
4.如果本条规定的任何义务已通过根据2016/679号条例第35条或2016/680号指令第27条进行的数据保护影响评估得到履行，则第1款提及的基本权利影响评估应与该数据保护影响评估一并进行。
5.人工智能办公室应开发一个问卷模板，包括通过一个自动工具，以方便用户以简化的方式履行本条规定的义务。

第4章
通知机关和通知机构

第30条
通知机关

1.每个成员国应指定或建立至少一个通知机关，负责制定和实施评估、指定和通知合格性评估机构及对其进行监督的必要程序。
2.成员国可决定第1款所述的评估和监测应由765/2008号条例所指的国家认证机构进行。
3.通知机关的设立、组织和运作方式应确保不与合格性评估机构发生利益冲突，并确保其活动的客观性和公正性。
4.通知机关的组织方式应使与合格性评估机构的通知有关的决定由不同于对这些机构进行评定的主管机关做出。
5.通知机关不得在商业或竞争基础上提供或提供合格性评估机构所从事的任何活动或任何咨询服务。
6.通知机关应根据第70条的规定为其获得的信息保密。
7.通知机关应配备足够数量的称职人员，以适当履行其任务。主管机关应酌情

具备其职能所需的信息技术、人工智能和法律等领域的专业知识，包括对基本权利的监督。

第31条
合格性评估机构的通知申请

1.合格性评估机构应向其所在成员国的通知机关提交通知申请。
2.通知申请应附有对合格性评估活动、合格性评估模块和合格性评估机构声称有能力胜任的人工智能系统的说明，以及由国家认证机构颁发的认证证明，如有，证明合格性评估机构符合第33条规定的要求。申请通知机关根据任何其他欧盟统一立法的现有指定相关的任何有效文件也应包括在内。
3.如果相关合格性评估机构无法提供认证证明，则应向通知机关提供所有必要的文件证据，以便对其是否符合第33条规定的要求进行核查、认可和定期监测。对于根据任何其他欧盟统一立法指定的通知机构，与这些指定相关的所有文件和认证可酌情用于支持本条例规定的指定程序。每当发生相关变化时，通知机构应更新第2款和第3款中提及的文件，以便负责通知机构的机关能够监测和核查对第33条规定的所有要求的持续的遵守情况。

第32条
通知程序

1.通知机关只能通知符合第33条要求的合格性评估机构。
2.通知机关应使用由欧盟委员会开发和管理的电子通知工具，将第1款提及的每一合格性评估机构的情况通知欧盟委员会和其他成员国。。
3.第2款所指的通知应包括合格性评估活动、合格性评估模块、有关的人工智能系统和相关能力证明的全部细节。如果通知不是以第31条第2款所述的认证证明为依据，则通知机关应向欧盟委员会和其他成员国提供书面证据，证明合格性评估机构的能力，以及为确保定期监测该机构并使其继续满足第33条规定的要求而做出的安排。
4.有关合格性评估机构只有在委员会或其他成员国在通知机关发出通知后两周内未提出反对意见，如果通知包括第31条第2款所述的认证证明，或在通知机关发出通知后两个月内未提出反对意见，如果通知包括第31条第3款所述的文件证据，方可开展通知机构的活动。
4a.如有异议，欧盟委员会应立即与相关成员国和合格性评估机构进行磋商。据此，委员会应决定授权是否合理。委员会应将其决定通知有关成员国和相关的合格性评估机构。

第33条
与通知机构有关的要求

1.通知机构应根据国家法律成立并具有法人资格。
2. 通知机构应满足完成任务所需的组织、质量管理、资源和流程要求，以及适当的网络安全要求。
3. 通知机构的组织结构、职责分配、报告关系和运作应足以确保对其开展的合

格性评估活动的绩效和结果有信心。
4. 通知机构应独立于其开展合格性评估活动的高风险人工智能系统的提供者。通知机构也应独立于在被评估的高风险人工智能系统中拥有经济利益的任何其他经营者，以及提供者的任何竞争对手。这并不排除使用合格性评估机构运作所必需的经评估的人工智能系统，或将此类系统用于个人目的。
4a. 合格性评估机构、其高层管理人员和负责执行合格性评估任务的人员不得直接参与高风险人工智能系统的设计、开发、营销或使用，也不得代表参与这些活动的各方。其不得从事任何可能有损于其独立判断或诚信的活动。这尤其适用于咨询服务。
5. 通知机构的组织和运作应保障其活动的独立性、客观性和公正性。通知机关应记录和实施保障公正性的结构和程序，并在其整个组织、人员和评估活动中促进和应用公正性原则。
6. 通知机构应制定有文件证明的程序，确保其人员、委员会、附属机构、分包商和任何相关机构或外部机构的人员按照第70条的规定对其在开展合格性评估活动期间掌握的信息保密，除非法律要求披露。通知机构的工作人员有义务对在执行本条例规定的任务过程中获得的所有信息保守职业秘密，但与开展活动的成员国的通知机关有关的信息除外。
7. 通知机构应制定开展活动的程序，这些程序应适当考虑到企业的规模、所处行业、结构以及有关人工智能系统的复杂程度。
8. 通知机构应为其合格性评估活动投保适当的责任险，除非责任由其所在的成员国根据国内法承担，或该成员国本身直接负责合格性评估。
9. 通知机构应能以最高程度的专业操守和特定领域的必要能力执行本条例赋予的所有任务，无论这些任务是由通知机构自己执行，还是由代表执行并由通知机构负责。
10. 通知机构应具备足够的内部能力，以便能够有效地评估外部各方代表其开展的任务。通知机关应长期拥有足够的行政、技术、法律和科学人员，这些人员应具备与相关类型的人工智能系统、数据和数据计算有关的经验和知识，并符合本编第2章所列的要求。
11. 通知机构应参与第38条所述的协调活动，还应直接参加或派代表参加欧洲标准化组织，或确保了解和掌握相关标准的最新情况。

第33a条
推定符合与通知机构有关的要求

如果合格性评估机构证明其符合相关统一标准或部分标准中规定的标准，而这些标准的参考文件已在《欧盟官方公报》上公布，则应推定该机构符合第33条规定的要求，只要适用的统一标准涵盖了这些要求。

第34条
通知机构的附属机构和分包

1. 如果通知机构分包与合格性评估有关的具体任务或求助于附属机构，则应确保分包商或附属机构符合第33条规定的要求，并应相应通知通知机关。
2. 通知机构应对分包商或子公司，无论其设立在何处，执行的任务负全部责

任。
3.只有在征得提供者同意的情况下，才可将活动分包或由子公司开展。通知机构应公布其附属1机构名单。
4.与分包商或附属机构的资格评估及其根据本条例开展的工作有关的文件，应自分包活动终止之日起5年内由通知机构保存。

第34a条
通知机构的业务义务

1. 通知机构应根据第43条所述的合格性评估程序，核查高风险人工智能系统是否符合要求。
2. 通知机构在开展活动时应避免给提供者造成不必要的负担，并适当考虑到企业的规模、所处行业、结构和有关高风险人工智能系统的复杂程度。尽管如此，通知机构仍应尊重高风险人工智能系统符合本条例要求所需的严格程度和保护水平。应特别注意尽量减少委员会2003/361/EC号建议中定义的微型和小型企业的行政负担和合规成本。
3. 通知机构应向第30条所述的通知机关提供并根据要求提交所有相关文件，包括提供者的文件，以便该机关开展评估、指定、通知、监测活动，并为本章所述的评估提供便利。

第35条
根据本条例指定的通知机构的识别号和名单

1.委员会应为通知机构分配一个标识号。即使一个机构根据多项联盟法案成为通知机构，委员会也应分配一个编号。
2.委员会应公布根据本条例通知的机构名单，包括分配给的标识号及其成为通知机关的活动。委员会应确保不断更新该名单。

第36条
通知变更

-1.通知机关应通过第32条第2款提及的电子通知工具，将与通知机构通知的任何相关变更通知委员会和其他成员国。
-1a.第31条和第32条所述的程序应适用于通知范围的扩大。对于除扩大范围以外的通知变更，应适用以下各款规定的程序。
如果通知机构决定停止其合格性评估活动，则应尽快通知通知机关和有关提供者，如果计划停止活动，则应在停止活动前一年通知。在通知机关停止活动后，认证可在九个月内临时有效，条件是另一个通知机构已书面确认其将承担这些认证所涵盖的人工智能系统的责任。新的通知机构应在该期限结束前完成对受影响的人工智能系统的全面评估，然后再为这些系统签发新的认证。如果通知机构已停止活动，通知机关应撤回指定。
1.如果通知机关有充分理由认为通知机构不再符合第33条规定的要求，或者认为通知机构未能履行其义务，通知机关应立即尽最大努力调查此事。在这种情况下，通知机关应将提出的反对意见通知有关通知机构，并使其有可能发表意

见。如果通知机关得出结论认为，通知机构不再符合第 33 条规定的要求，或未能履行其义务，则应根据未能符合这些要求或未能履行这些义务的严重程度，酌情限制、中止或撤回通知。通知机关应立即向欧盟委员会和其他成员国通报有关情况。
2a. 如果其指定被中止、限制或全部或部分撤回，通知机构应最迟在10天内通知有关制造商。
2b. 在限制、中止或撤回通知的情况下，通知机关应采取适当步骤，确保保存有关通知机构的档案，并应其他成员国的通知机关和市场监督管理机关的要求，向其提供这些档案。
2c. 在限制、中止或撤回指定的情况下，通知机关应：
a) 评估对通知机构颁发的认证的影响；
b) 在通知更改通知后的三个月内，向委员会和其他成员国提交调查结果报告；
c) 要求通知机构在主管机关确定的合理期限内，中止或撤回为确保市场上的人工智能系统具备合格性而不适当地发放的任何认证；
d) 向委员会和成员国通报其要求中止或撤回的认证；
e) 向提供者登记营业地所在成员国的国家主管机关提供其要求中止或撤回的认证的所有相关信息。该主管机关应在必要时采取适当措施，避免对健康、安全或基本权利造成潜在风险。
2d. 除不当签发的认证和通知被中止或限制的情况外，认证在以下情况下仍然有效：
a) 通知机关在中止或限制后一个月内确认，受中止或限制影响的认证不存在健康、安全或基本权利方面的风险，并且通知机关概述了补救中止或限制的时间表和预期行动；或
b) 通知机关已确认在中止或限制期间不会签发、修改或重新签发与中止有关的认证，并说明通知机构是否有能力在中止或限制期间继续监督和负责已签发的现有认证。如果负责通知机构的机关确定通知机构没有能力支持已签发的现有认证，则提供者应在中止或限制的三个月内，向认证所涉系统的提供者登记营业地所在成员国的国家主管机关提供一份书面确认，说明另一个合格的通知机构正在临时承担通知机构的职能，在中止或限制期间对认证进行监督并继续负责。
2e. 除不当签发的证明书和已撤回指定的证明书外，在下列情况下，证明书的有效期应为9个月：
a) 认证所涵盖的人工智能系统的提供者的登记营业地所在的成员国的国家主管机关已确认，有关系统对健康、安全和基本权利没有风险；以及
b) 认证所涵盖的人工智能系统的提供者的登记营业地所在的成员国的国家主管机关已确认，有关系统对健康、安全和基本权利没有风险。
b) 另一通知机构已书面确认将立即承担这些系统的责任，并将在撤回指定后12个月内完成对这些系统的评估。
在本款第一分段所述情况下，认证所涉系统的提供者营业地所在成员国的国家主管机关可将认证的临时有效期再延长3个月，但总共不得超过12个月。
2f. 受通知变更影响的国家主管机关或承担通知职能的通知机关应立即将此事通知欧盟委员会、其他成员国和其他通知机关。

第37条

对通知机关权限的质疑

1. 委员会应在必要时对有理由怀疑通知机关的能力或通知机关是否继续履行第33条规定的要求及其适用责任的所有情况进行调查。
2. 通知机关应根据要求向委员会提供与通知或保持有关通知机关的权限有关的所有相关信息。
3. 委员会应确保在根据本条进行调查过程中获得的所有敏感信息均按照第70条的规定予以保密。
4. 当欧盟委员会确定某一通知机关不符合或不再符合其通知要求时，应相应通知成员国，并要求其采取必要的纠正措施，包括必要时暂停或撤销通知。如果成员国未采取必要的纠正措施，委员会可通过实施法案中止、限制或撤销指定。该实施法案应根据第74条第2款所述审查程序通过。

第38条
通知机关的协调

1. 就高风险人工智能系统而言，欧盟委员会应确保在根据本条例开展合格性评估程序的通知机关之间建立适当的协调与合作，并以通知机关部门小组的形式适当运作。
2. 通知机关应确保其通知的机构直接或通过指定的代表参与该小组的工作。
2a. 委员会应促进成员国通知机关之间的知识和最佳实践交流。

第39条
第三国的合格性评估机构

根据与欧盟缔结了协议的第三国法律建立的合格性评估机构，只要符合第33条的要求或确保同等水平的合规性，就可以被授权开展本条例规定的通知机关的活动。

第5章
标准、合格性评估、认证、登记

第40条
统一标准和标准化交付成果

高风险人工智能系统若符合统一标准或其部分内容，且其参考文件已根据1025/2012号条例在《欧盟官方公报》上公布，则应推定为符合本编第2章规定的要求，或在适用的情况下，符合关于通用目的人工智能的章节规定的要求，只要这些标准涵盖了这些要求。
2. 委员会应根据1025/2012号条例第10条，在没有无故拖延的情况下，发出涵盖本条例第二编第3章和适用的关于通用目的人工智能的章节的所有规定的标准化请求。标准化申请还应要求提供有关报告和文件流程的可交付成果，以改善人工智能系统的资源性能，如减少高风险人工智能系统在其生命周期内的能源和其他资源消耗，以及有关通用人工智能模型的节能开发。在准备标准化要求

时，委员会应咨询欧洲人工智能委员会和利益相关方，包括咨询论坛。
在向欧洲标准化组织发出标准化要求时，欧盟委员会应规定标准必须一致，包括与附件二所列欧盟现行安全法规所涵盖产品的各部门现有和未来制定的标准一致，明确并旨在确保在欧盟市场上投放或投入使用的人工智能系统或模型符合本条例规定的相关要求。
委员会应要求欧洲标准化组织提供证据，证明其根据欧盟1025/2012号条例第24条的规定，为实现上述目标做出了最大努力。
1c 参与标准化进程的各方应努力促进人工智能领域的投资和创新，包括通过提高法律确定性以及联盟市场的竞争力和增长，并促进加强标准化方面的全球合作，同时考虑到人工智能领域符合联盟价值观、基本权利和利益的现有国际标准，并根据1025/2012号法规第5、6和7条，加强多利益相关方治理，确保利益的均衡代表和所有利益相关方的有效参与。

第41条
共同规格

1.委员会有权在与第58条提及的咨询论坛协商后，根据第74条第2款提及的审查程序，在满足以下条件的情况下，通过实施法案，为本条例范围内的人工智能系统制定本编第2章所列要求的共同规格，或在适用的情况下，制定关于通用目的人工智能的章节所列要求的共同规格：
(a) 根据第1025/2012号条例第10条第1款，欧盟委员会已要求一个或多个欧洲标准化组织起草本编第2章所列要求的统一标准；以及
(i) 申请未被任何欧洲标准化组织接受；或
(ii) 未在1025/2012号条例第10条第1款规定的期限内交付针对该请求的统一标准；或
(iii) 相关的统一标准没有充分解决基本权利问题；或
(iv) 统一标准不符合要求；以及
(b) 根据1025/2012号条例，《欧盟官方公报》尚未公布涉及本编第2章所述要求的统一标准的参考文件，且预计在合理期限内不会公布此类参考文件。
1a.在制定实施法草案之前，委员会应通知欧盟1025/2012号条例第22条所指的委员会，其认为第1款的条件已经满足。
3.高风险人工智能系统如符合第1款所述的共同规格或其部分内容，应推定为符合本编第2章所列的要求，只要这些共同规格涵盖了这些要求。
3a.如果欧洲标准化组织通过了一项统一标准，并建议欧盟委员会在《欧盟官方公报》上公布其参考文件，欧盟委员会应根据1025/2012号条例对该统一标准进行评估。当统一标准的参考文件在《欧盟官方公报》上公布时，欧盟委员会应废除第1款和第1b款提及的法案，或其中涉及本编第2章中相同要求的部分。
4.如果高风险人工智能系统的提供者不符合第1款所述的共同规格，则应充分说明其采用的技术解决方案至少达到了第2章所述的同等水平。
4b.当成员国认为一项共同规格不完全符合本编第2章规定的要求时，应将此情况通知委员会并做出详细解释，委员会应评估该信息，并酌情修订确立有关共同规格的实施法案。

第42条

推定符合特定要求

1.如果高风险人工智能系统经过训练和测试，其数据反映了拟使用该系统的特定地理、行为、场景或功能环境，则应推定该系统符合第10条第4款规定的各项要求。
2.根据欧洲议会和欧盟理事会2019/881号条例的网络安全计划认证或发布合格性声明的高风险人工智能系统，其参考文件已在《欧盟官方公报》上公布，应推定为符合本条例第15条规定的网络安全要求，只要网络安全认证或合格性声明或其部分内容涵盖这些要求。

第43条
合格性评估

1.对于附件三第1点所列的高风险人工智能系统，如果在证明高风险人工智能系统符合本编第2章规定的要求时，提供者采用了第40条所述的统一标准，或在适用的情况下采用了第41条所述的共同规格，则提供者应选择下列程序之一：
(a) 附件六中提及的基于内部控制的合格性评估程序；或
(b) 附件七所述的以质量管理体系评估和技术文件评估为基础的合格性评估程序，并有通知机关的参与。
在证明高风险人工智能系统符合本编第 2 章规定的要求时，在下列情况下，提供者应遵循附件七规定的合格性评估程序：
(a) 不存在第40条所述的统一标准，也不存在共同规格；
(aa) 提供者未应用或仅部分应用了统一标准；
(b) 存在第a点提及的共同规格，但提供者没有应用这些规格；
(c) 第a点提及的一项或多项统一标准在发布时受到限制，且仅限于标准中受到限制的部分；
就附件七所述的合格性评估程序而言，提供者可选择任何一个通知机构。但是，当执法、移民或庇护机关以及欧盟机构、团体或机关意图将该系统投入使用时，第63条第5款或第6款所述的市场监督管理机关，如适用，应充当通知机构。
2.对于附件三第2至第8点所述的高风险人工智能系统，提供者应遵循附件六所述的基于内部控制的合格性评估程序，该程序没有规定通知机构的参与。
3.对于附件二A节所列法令适用的高风险人工智能系统，提供者应按照这些法令的要求进行相关的合格性评估。本编第2章规定的要求应适用于这些高风险人工智能系统，并应成为评估的一部分。附件七第4.3、4.4、4.5点和第4.6点第5段也应适用。
为评估目的，已根据这些法案获得通知的通知机构应有权控制高风险人工智能系统是否符合本编第2章规定的合格性要求，条件是这些通知机构是否符合第33条第3款、第9款和第10款规定的要求已根据这些法案的通知程序进行了评估。
如果附件二A节所列的法律使得产品制造商能够选择不接受第三方合格性评估，但该制造商必须采用了涵盖所有相关要求的所有统一标准，而且还采用了涵盖本编第2章所列要求的统一标准或者，如适用，第41条所提及的共同规格，该制造商才可使用该选择权。

4. 已经接受过合格性评估程序的高风险人工智能系统，无论修改后的系统是意图进一步分发，还是由目前的部署者继续使用，只要进行实质性修改，就必须接受新的合格性评估程序。
对于投放市场或投入使用后仍在继续学习的高风险人工智能系统，如果提供者在初次合格性评估时已预先确定对高风险人工智能系统及其性能的更改，而且这些更改是附件四第2f点所述技术文件所载信息的一部分，则不应构成实质性修改。
5. 委员会有权根据第73条通过授权法案，以便根据技术进步更新附件六和附件七。
6. 委员会有权通过修改第1款和第2款的授权法案，以使附件三第2至第8点所指的高风险人工智能系统接受附件七或其部分内容所指的合格性评估程序。委员会在通过此类授权法案时，应考虑到附件六提及的基于内部控制的合格性评估程序在预防或最大限度地降低此类系统对健康和安全以及基本权利的保护所造成的风险方面的有效性，以及通知机构是否具备足够的能力和资源。

第44条
认证

1. 通知机构根据附件七签发的认证应使用通知机构所在成员国的有关机关易于理解的语言。
2. 认证的有效期为：附件二所列人工智能系统不超过五年，附件三所列人工智能系统不超过四年。根据提供者的申请，认证的有效期可根据适用的合格性评估程序进行重新评定后再延长，附件二所列的人工智能系统不超过五年，附件三所列的人工智能系统不超过四年。只要对认证进行补充的认证仍然有效，对认证的任何补充就仍然有效。
3. 如果通知机构发现特定人工智能系统不再符合本编第2章规定的要求，则应在考虑到成比例性原则的情况下，中止或撤回所颁发的认证或对其施加任何限制，除非该系统的提供者在通知机构规定的适当期限内采取了适当的纠正行动，以确保符合这些要求。通知机构应说明其决定的理由。

第45条
对通知机构的决定提出申诉

应具备针对通知机构决定的申诉程序，包括关于发布的合格性的决定。

第46条
通知机构的信息义务

1. 通知机构应向通知机关通报以下情况：
(a) 根据附件七的要求颁发的任何联盟技术文件评估认证、对这些认证的任何补 充、质量管理体系认证；
(b) 拒绝、限制、中止或撤回根据附件七的要求颁发的欧盟技术文件评估认证或质量管理体系认证；
(c) 影响通知范围或通知条件的任何情况；

(d) 从市场监督管理机关收到的关于提供合格性评估活动信息的任何要求；
(e) 应要求提供在其通知范围内开展的合格性评估活动和任何其他活动，包括跨境活动和分包活动。
2. 每个通知机构应将下列情况通知其他通知机构：
(a) 已拒绝、中止或撤回的质量管理体系认证，并应要求提供其已签发的质量体系认证；
(b) 已拒绝、撤回、中止或以其他方式限制的欧盟技术文件评估认证或其任何补充，并应要求提供其已签发的认证和/或补充。
3. 各通知机构应向其他开展类似合格性评估活动的通知机构提供有关负面合格性评估结果问题的相关信息，并应要求提供正面合格性评估结果的相关信息。
3a. 应按照第70条的规定履行第1至第3款所述义务。

第47条
合格性评估程序的克减

1. 通过对第43条的克减，并根据有正当理由的请求，任何市场监督管理机关可授权在有关成员国境内，出于公共安全或保护人的生命和健康、环境保护以及保护关键工业和基础设施资产的特殊原因，将特定的高风险人工智能系统投放市场或投入使用。考虑到克减的特殊原因，在进行必要的合格性评估程序期间，该授权应是有期限的。这些程序的完成不得无故拖延。
1a. 在出于公共安全的特殊原因或在自然人的生命或人身安全受到具体、实质性和迫在眉睫的威胁的情况下，执法机关或民防机关可在没有第1款所述授权的情况下，将特定的高风险人工智能系统投入使用，条件是在使用期间或之后申请此类授权，不得无故拖延；如果此类授权被拒绝，则应立即停止使用，并应立即弃置使用该系统的所有结果和产出。
2. 只有当市场监督管理机关认为高风险人工智能系统符合本编第2章的要求时，方可签发第1款所述授权。市场监督管理机关应将根据第1款签发的任何授权通知欧盟委员会和其他成员国。这项义务不包括与执法机关活动有关的敏感业务数据。
3. 如果在收到第2款所述信息后的15个日历日内，成员国或欧盟委员会均未对成员国市场监督管理机关根据第1款发出的授权提出异议，则应认为该授权是合理的。
4. 如果在收到第2款所述通知后的15个日历日内，一成员国对另一成员国市场监督管理机关签发的授权提出异议，或欧盟委员会认为该授权违反欧盟法律，或成员国关于第2款所述系统合规性的结论毫无根据，欧盟委员会应毫不迟延地与相关成员国进行磋商；应与相关经营者进行磋商，并使其有可能提出自己的意见。据此，委员会应决定授权是否合理。委员会应将其决定通知有关成员国和相关经营者。
5. 如果认为授权不合理，有关成员国的市场监督管理机关应撤回授权。
6. 对于与附件二A部分所述欧盟统一立法所涵盖产品有关的高风险人工智能系统，只适用该立法中规定的合格性评估克减程序。

第48条
欧盟合格性声明

1.提供者应为每个高风险人工智能系统起草一份书面的机器可读、实物或电子签名的欧盟合格性声明，并在人工智能高风险系统投放市场或投入使用后10年内将其交由国家主管机关保存。欧盟合格性声明应标明其所针对的高风险人工智能系统。欧盟合格性声明的副本应按要求提交给相关国家主管机关。
2.欧盟合格性声明应说明有关高风险人工智能系统符合本编第 2 章规定的要求。欧盟合格性声明应包含附件五所列信息，并应翻译为高风险人工智能系统投放市场或加以提供的成员国国家主管机关易于理解的语言。
3.如果高风险人工智能系统受制于其他欧盟统一立法，而这些立法也要求欧盟做出合格性声明，则应针对适用于高风险人工智能系统的所有欧盟立法，起草一份单一的欧盟合格性声明。该声明应包含识别声明所涉及的欧盟统一立法所需的所有信息。
4.通过起草欧盟合格性声明，提供者应承担起遵守本编第2章所列要求的责任。提供者应根据情况及时更新欧盟合格性声明。
5.欧盟委员会有权根据第73条通过授权法案，以更新附件五所列欧盟合格性声明的内容，从而引入因技术进步而变得必要的内容。

第49条
CE标识

1.CE合格性标识应遵循765/2008号条例第30条规定的一般原则。
1a.对于以数字方式提供的高风险人工智能系统，只有在可以通过人工智能系统的访问界面或通过易于访问的机器可读代码或其他电子手段轻松访问的情况下，才应使用数字CE标志。
2.对于高风险的人工智能系统，CE标志应明显、清晰且不可擦除地粘贴。如果由于高风险人工智能系统的性质而无法或不能保证这样做，则应酌情将CE标志贴在包装上或随附文件上。
3.在适用的情况下，CE标志后应加上负责第43条规定的合格性评估程序的指定机构的识别号。通知机构的识别号应由该机构自己贴上，或根据其指示由提供者或其授权代表贴上。在任何提及高风险人工智能系统符合CE标志要求的宣传材料中也应标明识别号。
3a.如果高风险人工智能系统受欧盟其它法律的管辖，而其它法律也规定必须加贴CE标志，则CE标志应表明高风险人工智能系统也符合其它法律的要求。

第51条
登记

在将附件三所列的高风险人工智能系统投放市场或投入使用之前，附件三第2点所指的高风险人工智能系统除外，提供者或授权代表，如适用，应在第60条所指的欧盟数据库中登记自己及其系统。
1a.在将人工智能系统投放市场或投入使用之前，如果提供者已根据第6条第2a款规定的程序得出结论认为该系统不属于高风险系统，则提供者或授权代表，如适用，应在第60条所述的欧盟数据库中登记自身和系统信息。
1b.在投入使用或使用附件三所列的高风险人工智能系统，附件三第2点所列的

高风险人工智能系统除外，之前，作为公共机关、机构或团体或代表其行事的人员的部署者应在第60条所述的欧盟数据库中自行登记、选择系统并登记其使用情况。
1c. 对于附件三第1、6 和 7点所述执法、移民、庇护和边境管制管理领域的高风险人工智能系统，第1至1b款所述登记应在第60条所述欧盟数据库的安全非公开的部分进行，并视情况仅包括以下信息：
- 附件八A节第1至9点，但第5a、7和8点除外
- 附件八B节第1至3点
- 附件八第X部分第1至第9点，第6和第7点除外
附件八a第1至5点，第4点除外。只有欧盟委员会和第63条第5款提及的国家机关可以访问欧盟数据库的这些受限制的部分。
1d. 附件三第2点所指的高风险人工智能系统应在国家层面登记。

第四编
特定人工智能系统和通用目的人工智能的提供者和部署者的透明度义务

第52条
特定人工智能系统和通用目的人工智能的提供者和部署者的透明度义务

1. 提供者应确保意图与自然人直接互动的人工智能系统的设计和开发方式应使有关自然人知道他们正在与一个人工智能系统互动，除非从一个合理知情、善于观察和谨慎的自然人的角度来看，考虑到使用的情况和场景，这一点是显而易见的。
这一义务不适用于法律授权用于侦查、预防、调查和起诉刑事犯罪的人工智能系统，但第三方的权利和自由应得到适当保障，除非这些系统可供公众举报刑事犯罪。
1a. 生成合成音频、图像、视频或文本内容的人工智能系统，包括通用目的人工智能系统的提供者应确保人工智能系统的输出以机器可读的格式进行标注，并且可检测其系人为生成或操纵。在技术可行的情况下，提供者应确保其技术解决方案是有效、可互操作、稳健和可靠的，同时考虑到不同类型内容的特殊性和局限性、实施成本以及相关技术标准中可能反映的公认的先进技术。
如果人工智能系统执行的是标准编辑的辅助功能，或没有实质性地改变部署者提供的输入数据或其语义，或经法律授权用于侦查、预防、调查和起诉刑事犯罪，则本义务不适用。
2. 情感识别系统或生物特征分类系统的部署者应将该系统的运行情况告知接触该系统的自然人，并根据适用的2016/679号条例、2016/1725号条例和2016/280号指令处理个人数据。这项义务不适用于用于生物特征分类和情感识别的人工智能系统，因为法律允许在遵守欧盟法律的前提下，在适当保障第三方权利和自由的情况下，检测、预防和调查刑事犯罪。
3. 人工智能系统的部署者在生成或操纵构成深度伪造的图像、音频或视频内容时，应披露该内容是人为生成或操纵的。本义务不适用于经法律授权用于侦查、预防、调查和起诉刑事犯罪的情况。如果内容构成明显具有艺术性、创造性、讽刺性、虚构类比的作品或节目的一部分，本款规定的透明度义务仅限于以不妨碍作品展示或欣赏的适当方式披露此类生成或篡改内容的存在。

如果人工智能系统生成或篡改的文本是为了向公众提供有关公共利益问题的信息而发布的，其部署者应披露该文本是人工生成或篡改的。这项义务不适用于以下情况：法律授权使用人工智能系统侦查、预防、调查和起诉刑事犯罪；人工智能生成的内容经过人工审核或编辑控制；自然人或法人对发布的内容负有编辑责任。
3a. 第1至第3款中所提及的信息最迟应在首次互动或接触时以清晰可辨的方式提供给相关自然人。信息应符合适用的无障碍要求。
4. 第1款、第2款和第3款不应影响本条例第三章规定的要求和义务，也不应影响欧盟或各国法律规定的人工智能系统用户的其他透明度义务。
4a. 人工智能办公室应鼓励和促进在联盟一级起草行为守则，以促进有效履行有关检测和标注人工生成或篡改内容的义务。欧盟委员会有权根据第52e条第6-8款规定的程序，通过实施法案批准这些行为守则。如果委员会认为行为守则不够充分，则有权根据第73条第2款规定的审查程序，通过一项实施法案，明确规定履行这些义务的共同规则。

第八A编
通用目的人工智能

第1章
分类规则

第52a条
将通用人工智能模型分类为具有系统风险的通用人工智能模型

1. 如果一个通用人工智能模型符合以下任何一项标准，则应将其归类为具有系统性风险的通用人工智能模型：
(a) 根据适当的技术手段和方法，包括指标和基准，对其影响能力进行评估；
(b) 根据委员会依职权做出的决定，或在科学小组提出有保留的警告后，认为通用人工智能模型具有与a点相同的能力或影响。
2. 根据第1款a点，当一个通用人工智能模型用于训练的累计计算量，以浮点运算（FLOPs）计，大于10^25时，应推定该模型具有高影响能力。
3. 委员会应根据第73条第2款通过授权法案，修订上文各款列出的阈值，并在必要时根据不断发展的技术，如算法的改进或硬件效率的提高，对基准和指标进行补充，以使这些阈值反映先进技术水平。

第52b条
程序

1. 如果通用人工智能模型符合第A条第1款第a点所述要求，有关提供者应没有拖延地通知委员会，无论如何应在满足这些要求或得知将满足这些要求后2周内通知委员会。通知应包括必要的信息，以证明相关要求已得到满足。如果委员会发现某个通用人工智能模型存在系统性风险，但没有接到通知，委员会可以决定将其指定为存在系统性风险的模型。
2. 符合第A条第1款第a点所述要求的通用人工智能模型的提供者可在其通知中提

出证据充分的论据，以证明在特殊情况下，尽管该模型符合上述要求，但由于其具体特点，该通用人工智能模型不存在系统风险，因此不应被归类为具有系统风险的通用人工智能模型。
3.如果委员会得出结论认为，根据第2款提交的论据没有得到充分证实，而且相关提供者无法证明通用人工智能模型因其具体特点而不存在系统性风险，则委员会应驳回这些论据，通用人工智能模型应被视为具有系统性风险的通用人工智能模型。
4.委员会可依职权或在科学小组根据第[科学小组对系统性风险的警示]条第1款第a点提出有条件的警示后，根据附件YY规定的标准，指定特定通用人工智能模型具有系统性风险。委员会有权根据第74条第2款的规定，通过授权法案明确和更新附件YY中的标准。
4a.对于根据第4款被指定为具有系统性风险的通用人工智能模型的提供者提出的合理请求，委员会应予以考虑，并可决定根据附件YY所列标准重新评估该通用人工智能模型是否仍可被视为具有系统性风险。这种请求应包含做出指定决定后出现的客观、具体和新的理由。提供者最早可在指定决定后六个月内提出重新评估申请。如果委员会在重新评估后决定维持指定为具有系统风险的通用人工智能模式，提供者可在该决定做出后最早六个月内申请重新评估。
5.欧盟委员会应确保公布具有系统性风险的通用人工智能模型清单，并不断更新该清单，同时不影响根据欧盟和国家法律尊重和保护知识产权以及商业机密信息或商业秘密的需要。

第2章
通用人工智能模型提供者的义务

第52c条
通用人工智能模型提供者的义务

1.通用人工智能模型的提供者应：
(a) 编制并不断更新该模型的技术文件，包括其培训和测试过程及其评估结果，其中至少应包含附件XX所列要素，以便应要求向人工智能办公室和国家主管机关提供；
(b) 编制、不断更新并向意图将通用人工智能模型纳入其人工智能系统的人工智能系统提供者提供信息和文件。在不影响根据欧盟和国家法律尊重和保护知识产权和商业机密信息或商业秘密的情况下，信息和文件应：
(i) 使人工智能系统的提供者能够很好地了解通用人工智能模型的能力和局限性，并遵守本条例规定的义务；以及
(ii) 至少包含附件XX所列内容；
(c) 制定一项尊重欧盟版权法的政策，特别是通过先进技术等手段，确定和尊重根据2019/790号指令第4条第3款表达的权利保留；
-2.第1款规定的义务，除第c和d项外，不适用于根据免费且开源许可向公众提供的人工智能模型的提供者，该许可允许获取、使用、修改和分发模型，其参数，包括权重、模型结构信息和模型使用信息，均向公众公开。这一例外不适用于具有系统风险的通用人工智能模型。
2.通用人工智能模型的提供者在根据本条例行使其权限和权力时，应与委员会

和国家主管机关进行必要的合作。
(d) 根据人工智能办公室提供的模板，就通用人工智能模型训练所用的内容起草一份足够详细的摘要，并公布于众；
3. 在统一标准公布之前，通用人工智能模型的提供者可以依靠第E条所指的行为守则来证明其遵守了第1款中的义务。遵守欧洲统一标准可推定提供者符合要求。具有系统性风险的通用人工智能模型的提供者如不遵守经批准的行为守则，应证明有其他适当的合规手段，供委员会批准。
4. 为便于遵守附件XX，特别是第2条第d和e点的规定，委员会应有权根据第73条通过授权法案，详细规定衡量和计算方法，以便提供可比较和可核查的文件。
4a. 根据第73条第2款的规定，委员会有权通过授权法案，根据不断发展的技术对附件XX和XY 进行修订。
4b. 根据本条规定获得的任何信息和文件，包括商业秘密，均应按照第70条规定的保密义务处理。

第52ca条（新）
授权代表

1. 在联盟市场上投放通用人工智能模型之前，在联盟之外设立的提供者应通过书面授权，指定一名在联盟内设立的授权代表，使其能够执行本条例规定的任务。
2. 授权代表应执行提供者授权中规定的任务。其应根据要求以联盟机构的官方语言之一向人工智能办公室提供一份授权副本。在本条例中，授权代表应有权执行以下任务：
a) 核实附件九a中规定的技术文件是否已经编制，以及提供者是否履行了第52条c款和第52条d款，如适用，规定的所有义务；
b) 在该模型投放市场后的10年内，为人工智能办公室和国家主管机关保存一份技术文件副本，以及指定授权代表的提供者的详细联系信息；
c) 在收到合理要求的情况下，向人工智能办公室提供所有必要的信息和文件，包括根据第a点所保存的信息和文件，以证明遵守了本编规定的义务；
d) 在人工智能办公室和国家主管机关提出合理要求后，就后者对具有系统性风险的通用人工智能模型采取的任何行动与之合作，包括当该模型被集成到在欧盟市场上销售或投入使用的人工智能系统中时；
3. 授权代表应有权在与确保遵守本条例有关的所有问题上，除提供者外，或代替提供者，接受人工智能办公室或国家主管机关的询问。
4. 如果授权代表认为或有理由认为提供者的行为违反了本条例规定的义务，则应终止授权。在这种情况下，授权代表也应立即将任务终止及其原因通知人工智能办公室。
5. 本条规定的义务不适用于通用人工智能模型的提供者，这些模型在免费且开源许可下向公众开放，允许获取、使用、修改和分发模型，其参数，包括权重、模型架构信息和模型使用信息也向公众开放，除非相应通用人工智能模型存在系统性风险。

第3章
具有系统风险的通用人工智能模型提供者的义务

第52d条
具有系统风险的通用人工智能模型提供者的义务

1.除C条所列义务外，具有系统风险的通用人工智能模型的提供者还应：
(a) 根据反映先进技术水平的标准化协议和工具进行模型评估，包括对模型进行对抗测试并记录在案，以识别和降低系统性风险；
(b) 评估和减轻联盟层面可能存在的系统性风险，包括因开发、投放市场或使用具有系统性风险的通用人工智能模型而产生的系统性风险的来源；
(c) 跟踪、记录并及时向人工智能办公室报告，并酌情向国家主管机关报告严重事 件的相关信息以及为解决这些问题可能采取的纠正措施；
(d) 确保对具有系统风险的通用人工智能模型和模型的物理基础设施提供足够水平的网络安全保护。
2.在统一标准公布之前，具有系统性风险的通用人工智能模型的提供者可以依靠E条所指的行为守则来证明遵守了第1款的义务。遵守欧洲统一标准可推定提供者符合要求。具有系统性风险的通用人工智能模型的提供者如不遵守经批准的行为守则，应证明有其他适当的合规手段，供委员会批准。
3.根据本条规定获得的任何信息和文件，包括商业秘密，均应按照第70条规定的保密义务处理。

第52e条
行为守则

1.人工智能办公室应鼓励和促进在联盟一级制定行为守则，作为促进本条例正确实施的要件之一，同时考虑到国际进路。
2.人工智能办公室和人工智能理事会应致力于确保行为守则涵盖，但不一定仅限于，第C条和第D条规定的义务，包括以下问题：
(a) 确保第C条第a和b项所指的信息根据市场和技术的发展不断更新的手段，以及确保 培训内容摘要足够详细的手段；
(b) 确定联盟一级系统性风险的类型和性质，适当时包括其来源；
(c) 在联盟一级评估和管理系统性风险的措施、程序和方式，包括有关文件。联盟一级系统性风险的评估和管理应与风险成比例，考虑到风险的严重性和可能性，并根据人工智能价值链上可能出现和实现这些风险的方式，考虑到应对这些风险的具体挑战。
3.人工智能办公室可邀请通用人工智能模型的提供者以及相关国家主管机关参与行为守则的起草工作。公民社会组织、行业、学术界和其他利益相关方，如下游提供者和独立专家，可支持这一进程。
4.人工智能办公室和欧洲人工智能委员会应致力于确保业务守则明确规定其具体目标，并包含承诺或措施，包括适当的关键绩效指标，以确保实现这些目标，并在联盟层面适当考虑所有相关方，包括受影响人员。
5.人工智能办公室可邀请所有通用人工智能模型提供者参加行为守则。对于不构成系统性风险的通用人工智能模型的提供者来说，这种参与应仅限于本条第2款第a项所预见的义务，除非他们明确宣布有兴趣加入完整的守则。
6.人工智能办公室应努力确保行为守则的参与者定期向人工智能办公室报告承

诺的履行情况和所采取的措施及其结果，包括酌情根据关键绩效指标进行衡量。关键绩效指标和报告承诺应考虑到不同参与者在规模和能力方面的差异。
7.人工智能办公室和欧洲人工智能委员会应定期监测和评估参与方实现行为守则目标的情况及其对正确实施本条例的贡献。人工智能办公室和欧洲人工智能委员会应评估行为守则是否涵盖第C条和D条规定的义务，包括本条第2款所列的问题，并应定期监督和评估其目标的实现情况。委员会应公布其对行为守则充分性的评估结果。委员会可通过实施法案决定批准行为守则，并使其在欧盟内普遍有效。这些实施法案应根据第74条第2款规定的审查程序通过。
8.人工智能办公室还应酌情鼓励和促进对行为守则的审查和调整，特别是根据新出现的标准进行审查和调整。人工智能办公室应协助对现有标准进行评估。
9.如果在本条例开始适用时，行为守则还不能最终确定，或者如果人工智能办公室认为根据第6款的规定，行为守则还不够充分，委员会可以通过实施法案，为履行第C条[第52c条]和第D条[第52d条]规定的义务提供共同规则，包括第2款规定的问题。

第五编
支持创新的措施

第53条
人工智能监管沙盒

1.成员国应确保其主管机关在国家一级建立至少一个人工智能监管沙盒，该沙盒应在生效24个月后开始运作。该沙盒也可与其他一个或多个成员国的主管机关联合建立。委员会可为人工智能监管沙盒的建立和运行提供技术支持、建议和工具。上段规定的义务也可以通过参与现有的沙盒来履行，只要这种参与能为参与的成员国提供同等水平的国家覆盖。
1a.还可在区域或地方一级或与其他成员国的主管机关联合建立更多的人工智能监管沙盒；
1b.欧洲数据保护监督员还可为欧盟各机构、团体和部门建立人工智能监管沙盒，并根据本章规定行使国家主管机关的职责和任务。
1c.成员国应确保第1款和第1a款提及的主管机关划拨足够的资源，以有效和及时地遵守本条规定。
在适当情况下，国家主管机关应与其他相关机关合作，并可允许人工智能生态系统内的其他行为者参与。
本条不应影响根据国内法或欧盟法设立的其他监管沙盒。成员国应确保监管这些其他沙盒的机构与国家主管机关之间开展适当程度的合作。
1d.根据本条例第53条第1款建立的人工智能监管沙盒，应按照第53条和第53a条的规定，提供一个可控的环境，以促进创新，并在根据潜在提供者和主管机关之间商定的具体沙盒计划将创新的人工智能系统投放市场或投入使用之前，在有限的时间内为其开发、培训、测试和验证提供便利。此类监管沙盒可包括在沙盒监督下的真实世界条件下进行测试。
1e.主管机关应酌情在沙盒中提供指导、监督和支持，以确定风险，特别是基本权利、健康和安全、测试、缓解措施方面的风险，以及这些措施在本条例义务和要求方面的有效性，并在相关情况下，确定在沙盒中受监督的其他欧盟和成

员国立法的有效性。
1f.主管机关应向提供者和潜在提供者提供有关监管期望以及如何履行本条例规定的要求和义务的指导。
应人工智能系统提供者或潜在提供者的要求，主管机关应提供在沙盒中成功开展活动的书面证明。主管机关还应提供一份退出报告，详细说明在沙盒中开展的活动以及相关结果和学习成果。提供者可通过合格性评估程序或相关市场监督活动使用这些文件来证明其遵守了本条例。在这方面，市场监督管理机关和通知机关应积极考虑国家主管机关提供的退出报告和书面证明，以便在合理范围内加快合规性评估程序。
1fa在不违反第70条保密规定的前提下，经沙盒提供者/潜在提供者同意，欧盟委员会和理事会有权获取退出报告，并在根据本条例执行任务时酌情予以考虑。如果提供者和潜在提供者以及国家主管部门明确同意，退出报告可通过本条提及的单一信息平台公开发布。
1g.建立人工智能监管沙盒应旨在促进实现以下目标：
a）提高法律确定性，以实现对本条例或（在相关情况下）其他适用的联盟和成员国立法的监管合规；
b）通过与参与人工智能监管沙盒的机构合作，支持分享最佳实践；
c）促进创新和竞争力，推动人工智能生态系统的发展；
d）促进循证的监管学习；
e）促进和加快人工智能系统进入欧盟市场，特别是由小微型企业（SMEs），包括初创企业提供的人工智能系统。
2.国家主管机关应确保，如果创新人工智能系统涉及个人数据处理或属于其他国家机关或提供或支持数据访问的主管机关的监管范围，则国家数据保护机关和这些其他国家机关应与人工智能监管沙盒的运行相关联，并在各自任务和权力范围内酌情参与对这些方面的监管。
3.人工智能监管沙盒不应影响主管机构的监督和纠正权力。
监督沙盒的机关，包括地区或地方一级的机关。在此类人工智能系统的开发和测试过程中发现的对健康、安全和基本权利的任何重大风险都应得到充分缓解。如果无法有效缓解风险，国家主管机关应有权暂时或永久中止测试过程，或中止参与沙盒，并将此决定通知人工智能办公室。国家主管机关应在相关立法范围内行使其监督权，在对特定人工智能沙盒项目执行法律规定时使用其自由裁量权，目的是支持联盟内的人工智能创新。
4.根据适用的欧盟和成员国责任法，人工智能监管沙盒中的提供者和潜在提供者仍应对在沙盒中进行的实验给第三方造成的任何损害负责。不过，只要潜在提供者遵守具体计划及其参与条款和条件，并真诚遵循国家主管机关提供的指导，机关将不会对违反本条例的行为处以行政罚款。如果负责其他欧盟和成员国立法的主管机关积极参与了对沙盒中人工智能系统的监督，并提供了合规指导，则不得对该立法处以行政罚款。
4b.在设计和实施人工智能监管沙盒时，应酌情促进国家主管机关之间的跨境合作。
5.国家主管机关应在理事会框架内协调其活动并开展合作。
5a.国家主管机关应向人工智能办公室和理事会通报沙盒的设立情况，并可请求支持和指导。人工智能办公室应公布计划中和现有的人工智能沙盒清单，并不断更新，以鼓励监管沙盒中的更多互动和跨境合作。

5b. 国家主管机关应向人工智能办公室和理事会提交年度报告，从人工智能监管沙盒设立一年后开始，然后每年提交，直至其终止，并提交最后报告。这些报告应提供有关这些沙盒的实施进展和结果的信息，包括最佳实践、事件、经验教训和有关其设置的建议，以及在相关情况下，有关本条例，包括其授权法案和实施法案，和其他在沙盒内监管的欧盟法律的适用和可能的修订。这些年度报告或摘要应在线向公众提供。
委员会在执行本条例规定的任务时，应酌情考虑年度报告。
6. 委员会应根据第55条第1款第c项，开发一个包含与沙盒有关的所有相关信息的单一专用界面，使利益相关方能够与监管沙盒互动，向主管机关提出查询请求，并就嵌入人工智能技术的创新产品、服务、商业模式的合规性寻求非约束性的指导。在相关情况下，委员会应积极主动地与国家主管机关进行协调。

第53A条
人工智能监管沙盒的模式和运作

为避免联盟内各行其是，委员会应通过一项实施法案，详细说明人工智能监管沙盒的建立、开发、实施、运行和监督方式。执行法案应包括有关以下问题的共同原则：
a) 参与人工智能监管沙盒的资格和选择；
b) 申请、参与、监测、退出和终止人工智能监管沙盒的程序，包括沙盒计划和退出报告；
c) 适用于参与者的条款和条件。
实施法案应确保
a) 监管沙盒向任何符合资格和选择标准的人工智能系统潜在提供者开放。进入监管沙盒的标准是透明和公平的，设立机关会在申请后3个月内通知申请人其决定；
b) 监管沙盒允许广泛、平等的参与，并能跟上参与需求；潜在提供者还可与用户和其他相关第三方合作提交申请；
c) 有关监管沙盒的模式和条件应尽可能支持国家主管机关灵活建立和运行其人工智能监管沙盒；
d) 小微型企业和初创企业可免费进入人工智能监管沙盒，但不影响国家主管机关以公平和成比例的方式收回特殊费用；
e) 通过沙盒的学习成果，促进潜在提供者履行本条例规定的合格性评估义务或自愿适用第69条提及的行为守则；
f) 监管沙盒促进人工智能生态系统中其他相关参与者的参与，如通知机关和标准化组织、小微型企业、初创企业、企业、创新者、测试和实验设施、研究和实验实验室以及数字创新中心、卓越中心、个人研究者，以允许和促进与公共和私营部门的合作；
g) 申请、选择、参与和退出沙盒的程序、流程和行政要求简单、易懂、沟通清晰，以方便法律和行政能力有限的小微型企业和初创企业参与，并在整个欧盟范围内进行简化，以避免各行其是，并确保在欧盟范围内，参与由成员国或由教育部门设立的监管沙盒得到相互和统一的认可，并具有相同的法律效力；
h) 参与人工智能监管沙盒的期限应与项目的复杂性和规模相适应。国家主管部门可延长该期限；

i) 沙盒应促进工具和基础设施的开发，以测试、设定基准、评估和解释与监管学习相关的人工智能系统的各个层面，如准确性、稳健性和网络安全，以及降低基本权利、环境和整个社会风险的措施。
3. 沙盒中的潜在提供者，特别是小微型企业和初创企业，应在相关情况下被引导至部署之前的服务，如本条例的实施指导，以及其他增值服务，如标准化文件和认证、测试和实验设施、数字枢纽、卓越中心和欧盟基准能力方面的帮助。
4. 当国家主管机关考虑授权在根据本条设立的人工智能监管沙盒框架内进行真实世界条件下的测试时，它们应与参与者具体商定此类测试的条款和条件，特别是适当的保障措施，以保护基本权利、健康和安全。在适当情况下，他们应与其他国家主管机关合作，以确保整个联盟的实践一致。

第54条
进一步处理个人数据，以便在人工智能监管沙盒中为公众利益开发某些人工智能系统

1. 在人工智能监管沙盒中，为其他目的合法收集的个人数据，在满足以下所有条件的情况下，可以仅为开发、培训和测试沙盒中的某些人工智能系统而进行处理：
(a) 人工智能系统应由公共机关或受公法或私法管辖的另一自然人或法人在以下一个或多个领域为维护重大公共利益而开发：
(ii) 公共安全和公共卫生，包括疾病检测、诊断、预防、控制和治疗，以及改善卫生保健系统；
(iii) 高度保护和改善环境质量、保护生物多样性、污染以及绿色转型、减缓和适应气候变化；
(iiia) 能源的可持续性；
(iiib) 运输系统和流动性、关键基础设施和网络的安全性和韧性；
(iiic) 公共行政和公共服务的效率和质量；
(b) 所处理的数据是遵守第三编第2章中提及的一项或多项要求所必需的，而这些要求无法通过处理匿名化、合成或其他非个人数据来有效满足；
(c) 具备有效的监测机制，以确定在沙盒实验期间是否可能出现2016/679号条例第35条和2018/1725号条例第39条所述的对数据主体的权利和自由的任何高风险，以及及时降低这些风险并在必要时停止处理的响应机制；
(d) 沙盒中将要处理的任何个人数据均处于功能独立、隔离和受保护的数据处理环境中，由潜在提供者控制，且只有获得授权的人才能访问这些数据；
(e) 提供者只能根据欧盟数据保护法进一步共享原始收集的数据。在沙盒中收集的任何个人数据都不能在沙盒之外共享
(f) 沙盒中对个人数据的任何处理都不会导致影响数据主体的措施或决定，也不会影响其在欧盟个人数据保护法中规定的权利的适用；
(g) 通过适当的技术和组织措施保护在沙盒中处理的任何个人数据，并在沙盒参与终止或个人数据保存期结束后删除这些数据；
(h) 除非欧盟或国家法律另有规定，沙盒中的个人数据处理日志在参与沙盒期间保留；
(i) 完整、详细地说明人工智能系统的培训、测试和验证过程及原理，并将测

试结果作为附件四技术文件的一部分；
(j) 在主管机关网站上公布在沙盒中开发的人工智能项目、其目标和预期成果的简短摘要。这项义务不包括与执法、边境管制、移民或庇护机关的活动有关的敏感业务数据。
1a. 为了预防、调查、侦查或起诉刑事犯罪或执行刑事处罚，包括保障和预防对公共安全的威胁，在执法机关的控制和负责下，人工智能监管沙盒中的个人数据处理应基于特定的成员国或联盟法律，并受制于第1款所述的相同累积条件。
2. 第1款不妨碍欧盟或成员国立法排除为该立法明确提及的目的之外的其他目的进行处理，也不妨碍欧盟或成员国法律规定为开发、测试和培训创新人工智能系统或任何其他法律依据所必需的个人数据处理依据，并符合欧盟关于保护个人数据的法律。

第54a条
在人工智能监管沙盒之外的真实环境中测试高风险人工智能系统

1. 附件三所列高风险人工智能系统的提供者或潜在提供者可根据本条规定和本条所述真实世界测试计划，在人工智能监管沙盒之外的真实世界条件下对人工智能系统进行测试，但不影响第5条的禁止规定。
真实世界测试计划的详细内容应在委员会根据第74条第2条所述审查程序通过的实施法案中具体规定。
本规定不影响欧盟或各国关于在实际条件下对附件二所列法规所涵盖产品的高风险人工智能系统进行测试的法律。
2. 提供者或潜在提供者可自行或与一个或多个潜在部署者合作，在人工智能系统投放市场或投入使用之前的任何时候，在真实世界条件下对附件三所述高风险人工智能系统进行测试。
3. 根据本条规定在真实世界条件下对高风险人工智能系统进行的测试，不得妨碍国家或联盟法律可能要求的伦理审查。
4. 医疗服务提供者或潜在医疗服务提供者只有在满足以下所有条件的情况下，才能在真实世界的条件下进行测试：
(a) 提供者或潜在提供者已制定真实世界测试计划，并提交给将在真实世界条件下进 行测试的成员国的市场监督管理机关；
(b) 拟进行真实情况下的测试的成员国的市场监督管理机关已批准真实情况下的测试和真实情况下的测试计划。如果该成员国的市场监督管理机关在 30 天内未做出答复，则应将真实情况下的测试和真实情况下的测试计划理解为已获批准。在国家法律未规定默许的情况下，真实世界条件下的测试应获得授权；
(c) 提供者或潜在提供者，附件三第1、6 和7点所述执法、移民、庇护和边防管理领域的高风险人工智能系统以及附件三第2点所述的高风险人工智能系统除外，已在第60条第3款所述欧盟数据库的非公开部分登记了真实世界条件下的测试，并提供了欧盟唯一的单一识别码和附件八a中规定的信 息。
(d) 在真实世界条件下进行检测的提供者或潜在提供者已在欧盟设立机构，或已指定在欧盟设立机构的法律代表；
(e) 为在真实世界条件下进行测试而收集和处理的数据，只能在执行欧盟法律规定的适当且适用的保障措施下才能传输到第三国；
(f) 在真实世界条件下的测试时间不超过实现其目标所需的时间，在任何情况

下不超过6个月，可再延长6个月，但提供者须事先通知市场监督管理机关，并说明延长时间的必要性；
(g) 因年龄、身体或精神残疾而属于弱势群体的人得到适当保护；
(h) 如果提供者或潜在提供者与一个或多个潜在部署者合作组织真实世界条件下的测试，后者已被告知与其参与决定相关的测试的所有方面，并获得了关于如何使用第13条所述人工智能系统的相关说明；提供者或潜在提供者和部署者应缔结协议，明确各自的作用和责任，以确保遵守本条例以及其他适用的欧盟和成员国立法中关于真实世界条件下测试的规定；
(i) 在真实世界条件下的测试对象已根据第54b条的规定表示知情同 意，或在执法情况下，如果征求知情同意会妨碍人工智能系统的测 试，则测试本身和在真实世界条件下的测试结果不得对测试对象产 生任何负面影响，其个人资料应在测试完成后被删除。
(j) 提供者或潜在提供者和部署者对真实情况下的测试进行有效监督，这些人员在相关领域具有适当资格，并具备执行任务所需的能力、培训和授权；
(k) 可以有效地推翻和忽略人工智能系统的预测、建议或决定。
5. 任何在真实世界条件下进行测试的对象或视情况而定，其合法指定的代表均可随时撤销其知情同意并要求立即永久删除其个人数据，从而退出测试，而不会因此受到任何损害，也无需提供任何理由。撤销知情同意不会影响已经开展的活动。
5a. 根据第63a条，成员国应授权其市场监督管理机关要求提供者和潜在提供者提供信息，进行事先没有通知的远程或现场检查，并对在真实世界条件下开展的测试和相关产品进行检查。市场监督管理机关应利用这些权力确保这些测试的安全发展。
6. 在真实情况下的测试过程中发现的任何严重事故，应根据本条例第62条向国家市场监督管理机关报告。提供者或潜在提供者应立即采取缓解措施，如未采取缓解措施，则应暂停真实情况下的测试，直至采取缓解措施或终止测试。提供者或潜在提供者应制定程序，以便在终止真实情况下的测试后立即召回人工智能系统。
7. 提供者或潜在提供者应将暂停或终止真实条件下的检测以及最终结果通知拟进行真实条件下检测的成员国的国家市场监督管理机关。
8. 提供者和潜在提供者应根据适用的欧盟和成员国责任法，对其在参与真实情况下的测试过程中造成的任何损害承担责任。

第54b条
知情同意参与人工智能监管沙盒之外真实世界条件下的测试

1. 为了根据第54a条的规定在真实世界的条件下进行测试，测试对象应在参加测试之前，并在得到有关以下方面的简明、清楚、相关和易懂的信息之后，自由地表示知情同意：
(i) 在真实世界条件下进行测试的性质和目的，以及参加测试可能带来的不便；
(ii) 在真实世界条件下进行测试的条件，包括测试主体参与测试的预期时间；
(iii) 测试主体参与测试的权利和保障，特别是其拒绝参与测试的权利和随时退出真实 环境测试的权利，而不会因此受到任何损害，也无需提供任何理由；

(iv) 要求推翻或忽略人工智能系统的预测、建议或决定的方式；
(v) 根据第54a条第4c款的规定，在真实世界条件下进行检测的联盟范围内的单一识别号，以及提供者或其法定代表的详细联系方式，可向其索取进一步信息。
2.知情同意书应注明日期并记录在案，副本应交给测试主体或其法定代理人。

第55条
针对提供者和部署者，特别是小微型企业，包括初创企业的措施

1.成员国应采取以下行动
(a) 为在欧盟拥有登记办公室或分支机构的小微型企业（包括初创企业）提供优先进入人工智能监管沙盒的机会，只要它们满足资格条件和选择标准。只要符合资格条件和遴选标准，优先准入不应排除第一项所述以外的其他小微型企业，包括初创企业，进入人工智能监管沙盒；
(b) 针对小微型企业，包括初创企业，用户以及适当情况下的地方公共机关的需要，就本条例的应用组织具体的提高认识和培训活动；
(c) 利用现有的专门渠道，并酌情建立新的渠道，与包括初创企业在内的小微型企业、用户、其他创新者以及适当的地方公共机关进行沟通，就本条例的实施提供建议并回答询问，包括参与人工智能监管沙盒；
(ca) 促进小微型企业和其他相关利益方参与标准化制定过程。
2.在根据第43条规定确定合格性评估费用时，应考虑到小微型企业，包括初创企业，的具体利益和需求，并根据其规模、市场大小和其他相关指标按比例降低这些费用。
2a.人工智能办公室应采取以下行动：
(a) 应欧洲人工智能委员会的要求，提供本条例所涉领域的标准化模板；
(b) 开发并维护一个单一的信息平台，为联盟内所有运营商提供与本条例相关的易于使用的信息；
(c) 组织适当的宣传活动，提高人们对本条例规定的义务的认识；
(d) 评估和促进公共采购程序中与人工智能系统有关的最佳实践的趋同。

第55a条
特定运营者的克减

2b.欧盟委员会关于微型、小型和中型企业定义的2003/361/EC号建议附件第2条第3款所定义的微型企业，只要这些企业没有同一附件第3条所定义的合伙企业或关联企业，可以通过简化的方式履行本条例第17条所要求的质量管理体系的某些要素。为此，欧盟委员会应在不影响保护水平和遵守高风险人工智能系统要求的前提下，考虑微型企业的需要，制定关于可以简化方式满足的质量管理系统要素的指南。
2c.第1款不得解释为免除这些经营者履行本条例规定的任何其他要求和义务，包括第9、10、11、12、13、14、15、61和62条规定的要求和义务。

第六编
治理

第55b条
联盟层面的治理

1.欧盟委员会应发展欧盟在人工智能领域的专业知识和能力。为此，委员会决定成立欧洲人工智能办公室。
2.成员国应为本条例所规定的委托给人工智能办公室的任务提供便利。

第1章
欧洲人工智能委员会

第56条
欧洲人工智能委员会的设立和结构

1.成立“欧洲人工智能委员会”。
2. 欧洲人工智能委员会应由每个成员国的一名代表组成。欧洲数据保护监督员应作为观察员参加。人工智能办公室也应出席委员会会议，但不参与表决。如果讨论的问题与其他国家和欧盟机关、机构或专家相关，欧洲人工智能委员会可根据具体情况邀请其参加会议。
2a.每位代表由其成员国指定，任期3年，可连任一次。
2b.成员国应确保其在欧洲人工智能委员会中的代表
(a) 在其成员国中拥有相关的权限和权力，以便为实现第58条所述欧洲人工智能委员会的任务做出积极贡献；
(b) 被指定为欧洲人工智能委员会的单一联络点，并根据成员国的需要，在必要时被指定为利益相关方的单一联络点；
(c) 有权促进其成员国国家主管机关在执行本条例方面的一致性和协调性，包括通过收集相关数据和信息来完成其在欧洲人工智能委员会的任务。
3.成员国指定的代表应以三分之二多数通过欧洲人工智能委员会的议事规则。议事规则应特别规定遴选程序、任期、主席的具体任务、表决方式以及欧洲人工智能委员会及其分组的活动安排。
3a. 欧洲人工智能委员会应设立两个常设分组，分别为市场监督管理机关和通知机关提供一个就市场监督和通知机关相关问题进行合作与交流的平台。
市场监管常设分组应作为2019/1020号条例第30条所指的本条例的行政合作组（ADCO）。
欧洲人工智能委员会可酌情设立其他常设或临时分组，以审议具体问题。在适当情况下，可邀请第XX条提及的咨询论坛的代表以观察员身份参加这些分组的具体会议。
3b. 欧洲人工智能委员会的组织和运作应确保其活动的客观性和公正性。
4 欧洲人工智能委员会应由成员国的一名代表担任主席。欧洲人工智能办公室应为委员会提供秘书处，根据主席的要求召开会议，并根据本条例及其议事规则规定的欧洲人工智能委员会任务拟定议程。

第58条
欧洲人工智能委员会的任务

欧洲人工智能委员会应向欧盟委员会和成员国提供建议和协助，以促进本条例的一致和有效实施。为此，欧洲人工智能委员会尤其可以
(a) 促进负责实施本条例的国家主管机关之间的协调，并在有关市场监督管理机关的合作和同意下，支持第63条第7a款所述市场监督管理机关的联合活动；
(b) 在成员国之间收集和分享技术和监管方面的专门知识和最佳实践；
(c) 为本条例的实施提供建议，特别是在通用人工智能模型规则的执行方面；
(d) 促进成员国行政管理实践的统一，包括第47条提及的合格性评估程序的克减、第53、54和54a条提及的监管沙盒的运作和真实世界条件下的测试；
(e) 应委员会的要求或主动就与本条例的实施及其一致和有效适用有关的任何事项提出建议和书面意见，包括
(i) 根据本条例及委员会的指引，制定及适用行为守则；
(ii) 根据第84条对本条例进行评估和审查，包括第62条提及的严重事件报告和第60条提及的数据库的运作情况，拟定授权法案或实施法案，以及使本条例与附件二所列法案保持一致的可能性；
(iii) 关于第三编第2章所列要求的技术规格或现有标准、
(iv) 第40条和第41条提及的统一标准或共同规格的使用、
(v) 各种趋势，如欧洲在人工智能领域的全球竞争力、欧盟对人工智能的吸收以及数字技能的发展；
(via) 人工智能价值链类型不断演变的趋势，特别是由此产生的对责任的影响；
(vi) 根据第7条对附件三进行修正的潜在必要性，以及根据第84条对第5条进行可能的修订的潜在必要性，同时考虑到相关的现有证据和先进技术的水平；
(f) 支持委员会促进人工智能素养，提高公众对使用人工智能系统的好处、风险、保障措施以及权利和义务的认识和了解；
(g) 促进共同准则的制定以及市场经营者和主管机关对本条例规定的相关概念的共 同理解，包括促进基准的制定；
(h) 酌情与其他联盟机构、机关、办公室和机构以及相关的联盟专家组和网络开展合作，特别是在产品安全、网络安全、竞争、数字和媒体服务、金融服务、消费者保护、数据和基本权利保护等领域；
(i) 促进与第三国主管机关和国际组织的有效合作；
(j) 协助国家主管机关和委员会发展实施本条例所需的组织和技术专长，包括协助评估参与实施本条例的成员国工作人员的培训需求；
(j1) 协助人工智能办公室支持国家主管机关建立和发展监管沙盒，并促进监管沙盒之间的合作和信息共享；
(k) 为指导文件的编制做出贡献并提供相关建议；
(l) 就人工智能方面的国际事务向委员会提供咨询意见。
(m) 就通用人工智能模型的合格警报向委员会提供意见；
(n) 听取成员国对通用人工智能模型的合格警告以及各国在人工智能系统，特别是集成通用人工智能模型的系统的监测和执行方面的经验和实践的意见。

第58a条
咨询论坛

1.应设立一个咨询论坛，向欧洲人工智能委员会和委员会提供咨询意见和技术知识，以帮助它们完成本条例规定的任务。
2.咨询论坛的成员应均衡地代表各利益相关方，包括工业界、初创企业、小微型企业、公民社会和学术界。咨询论坛的成员应兼顾商业和非商业利益，在商业利益类别中兼顾小微型企业和其他企业。
3.委员会应根据前款规定的标准，从在人工智能领域具有公认专长的利益相关方中任命咨询论坛的成员。
4.咨询论坛成员的任期为两年，最多可延长四年。
5.基本权利机构、欧洲联盟网络安全局、欧洲标准化委员会（CEN）、欧洲电工技术标准化委员会（CENELEC）和欧洲电信标准协会（ETSI）应为咨询论坛的常任成员。
6.咨询论坛应制定其议事规则。论坛应根据第2款规定的标准，从其成员中选出两名共同主席。共同主席的任期为两年，可连任一次。
7.咨询论坛每年至少举行两次会议。咨询论坛可邀请专家和其他利益相关方参加会议。
8.在履行第1款规定的职责时，咨询论坛可应欧洲人工智能委员会或委员会的要求，准备意见、建议和书面材料。
9.咨询论坛可酌情设立常设或临时分组，以审议与本条例目标有关的具体问题。
10.咨询论坛应编写其活动的年度报告。该报告应予以公布。

第1a章
独立专家科学小组

第58b条
独立专家科学小组

1.委员会应通过一项实施法案，对建立一个由独立专家组成的科学小组（“科学小组”）做出规定，以支持本条例规定的执法活动。这些实施法案应根据第74条第2款提及的审查程序通过。
2.科学小组应由委员会根据第3款所述任务所需的人工智能领域最新科学或技术知识挑选出的专家组成，并应能证明符合以下所有条件：
(a) 人工智能领域的专门知识和能力以及科学或技术专长；
(b) 独立于任何人工智能系统或通用人工智能模型或系统的提供者；
(c) 认真、准确和客观地开展活动的能力。委员会应与欧洲人工智能委员会协商，根据需要确定专家小组的专家人数，并应确保性别和地域的公平代表性。
3.科学小组应向欧洲人工智能办公室提供建议和支持，特别是在以下任务方面：
(a) 在通用人工智能模型和系统方面，支持本条例的实施和执行，特别是通过以下方式
(i) 根据第[科学小组对系统风险的警报]条的规定，就联盟层面通用人工智能模型可能存在的系统风险向人工智能办公室发出警报；
(ii) 促进开发评估通用人工智能模型和系统能力的工具和方法，包括通过基准；

(iii) 就具有系统风险的通用人工智能模型的分类提供建议；
(iv) 促进工具和模板的开发。
(b) 应市场监督管理机关的要求，支持其工作；
(c) 支持第63条第7a款所述的跨境市场监督活动，但不损害市场监督管理机关的权力；
(d) 根据第66条的规定，支持人工智能办公室履行其在保障条款方面的职责；
4. 专家应公正、客观地执行任务，并确保对执行任务和开展活动过程中获得的信息和数据保密。他们在执行第3款规定的任务时，不得寻求或接受任何人的指示。每位专家都应起草一份利益申报表，并公布于众。人工智能办公室应建立积极管理和防止潜在利益冲突的制度和程序。
5. 第1款提及的执行法案应包括关于科学小组及其成员发出警报和请求人工智能办公室协助其执行任务的条件、程序和方式的规定。

第58c条
成员国利用专家库的机会

1. 成员国可要求科学小组的专家支持其根据本条例开展的执法活动。
2. 成员国可能需要为专家的咨询和支持支付费用。酬金的结构和水平以及可收回费用的规模和结构应在第58b条第1款提及的实施法案中加以规定，同时应考虑到充分实施本条例的目标、成本效益以及确保所有成员国都能有效地获得专家服务的必要性。
3. 欧盟委应根据需要为成员国及时获得专家提供便利，并确保欧盟人工智能测试支持根据第68a条和专家根据本条开展的支持活动的组合得到有效的组织，并尽可能提供最佳的附加值。

第2章
国家主管机关

第59条
指定国家主管机关和单一联络点

2. 各成员国应为本条例之目的设立或指定至少一个通知机关和至少一个市场监督管理机关作为国家主管机关。这些国家主管机关应独立、公正和不带偏见地行使权力，以维护其活动和任务的客观性原则，并确保本条例的适用和实施。这些机构的成员不得采取任何与其职责不符的行动。在遵守这些原则的前提下，这些活动和任务可根据成员国的组织需要，由一个或多个指定的机构来完成。
3. 成员国应向委员会通报通知机关和市场监督管理机关的身份、这些机关的任务以及随后的任何变动。成员国应在本条例生效之日后12个月内，通过电子通信手段公布有关如何与主管机关和单一联络点取得联系的信息。成员国应指定一个市场监督管理机关作为本条例的单一联络点，并将单一联络点的身份通知欧盟委员会。欧盟委员会应公布单一联络点名单。
4. 成员国应确保向国家主管机关提供充足的技术、财政和人力资源以及基础设施，以有效履行本条例规定的任务。特别是，国家主管机关应长期拥有足够数

量的人员，其能力和专业知识应包括对人工智能技术、数据和数据计算、个人数据保护、网络安全、基本权利、健康和安全风险的深入了解，以及对现有标准和法律要求的了解。成员国应每年评估并在认为必要时更新本段所述的能力和资源要求。
4a. 国家主管机关应采取适当水平的网络安全措施。
4c. 国家主管机关在执行任务时，应遵守第70条规定的保密义务。
5. 成员国应在本条例生效后的一年内，并在此后每两年向委员会报告国家主管机关的财力和人力资源状况，并评估其是否充足。委员会应将这些信息转交欧洲人工智能委员会讨论并提出可能的建议。
6. 委员会应促进各国主管机关之间的经验交流。
7. 国家主管机关可酌情考虑欧洲人工智能委员会和委员会的指导和建议，就本条例的实施提供指导和建议，特别是向包括初创企业在内的小微型企业提供指导和建议。当国家主管机关意图就其他欧盟立法所涵盖领域的人工智能系统提供指导和建议时，应酌情咨询该欧盟立法下的国家主管机关。
8. 当联盟机构、机关和团体属于本条例的适用范围时，欧洲数据保护监督员应作为主管机关对其进行监督。

第七编
附件三所列的欧盟高风险人工智能系统的数据库

第60条
附件三所列的欧盟高风险人工智能系统的数据库

1. 欧盟委员会应与成员国合作，建立并维护一个欧盟数据库，其中包含第2款和第2a款提及的关于第6条第2款提及的根据第51条和第54a条登记的高风险人工智能系统的信息。在确定该数据库的功能规格时，委员会应咨询相关专家；在更新该数据库的功能规格时，委员会应咨询人工智能委员会。
2. 附件八A部分所列数据应由提供者或授权代表，如适用，录入欧盟数据库。
2a. 根据第51条第1a款和第1b款，附件八B节所列数据应由公共机关、机构或团体的部署者或其代表输入欧盟数据库。
3. 除第 51条第1c款和第54a条第5款提及的部分外，根据第51条登记的欧盟数据库中的信息应以方便用户的方式向公众提供。信息应易于浏览和机器可读。根据第54a条登记的信息应仅向市场监督管理机关和欧盟委员会开放，除非潜在提供者或提供者同意将该信息也向公众开放。
4. 欧盟数据库应仅包含根据本条例收集和处理信息所必需的个人数据。这些信息应包括负责登记系统并拥有代表提供者或部署者，如适用，的法律授权的自然人的姓名和联系方式。
5. 欧盟委员会是欧盟数据库的控制者。其应向提供者、潜在提供者和部署者提供充分的技术和行政支持。数据库应符合适用的无障碍要求。

第八编
后市场监测、信息共享、市场监督

第1章

后市场监测

第61条
提供者对高风险人工智能系统的后市场监测和后市场监测计划

1.提供者应以与人工智能技术的性质和高风险人工智能系统的风险成比例的方式，建立并记录后市场监测系统。
2.后市场监测系统应积极和系统地收集、记录和分析可能由部署者提供的或可能通过其他来源收集的关于高风险人工智能系统在整个寿命期间的性能的相关数据，并使提供者能够评价人工智能系统是否持续符合第三编第2章规定的要求。在相关情况下，后市场监测应包括分析与其他人工智能系统的相互作用。这项义务不应涵盖作为执法机关的部署者的敏感操作数据。
3.后市场监测系统应以后市场监测计划为基础。后市场监测计划应作为附件四所述技术文件的一部分。欧盟委员会应在本条例生效前6个月通过一项实施法案，详细规定后市场监测计划的模 板和计划应包括的内容清单。
4.对于附件二A部分所述法案所涵盖的高风险人工智能系统，如果已根据该立法建立了后市场监测系统和计划，为确保一致性、避免重复和尽量减少额外负担，提供者应可选择酌情使用第3款所述模板，将第1、2和3段所述必要内容纳入附件二A部分所列欧盟统一立法下的现有系统和计划，但须达到同等保护水平。
第一项也适用于附件三第5点所述的高风险人工智能系统，这些系统由须遵守欧盟金融服务立法对其内部管理、安排或流程要求的金融机构投放市场或投入使用。

第2章
共享严重事件的信息

第62条
严重事件的报告

1.在欧盟市场上销售的高风险人工智能系统的提供者应向发生事故的成员国市场监督管理机关报告任何严重事故。
1a.作为一般规则，第1款所述的报告期限应考虑到严重事件的严重性。
1b.第1款所述通知应在提供者确定人工智能系统与严重事故之间的因果关系或确定存在这种关系的合理可能性之后立即发出，而且无论如何不得迟于提供者或者，如适用，部署者意识到严重事故之后15天。
1c.尽管有第1b款的规定，如果发生第3条第44项第b点定义的大范围违规或严重事件，应立即提交第1款所述的报告，且不得迟于提供者或者，如适用，部署者意识到该事件后的两天。
1d.尽管有第1b款的规定，如果发生人员死亡事件，应在提供者或部署者确定，或者一旦怀疑高风险人工智能系统与严重事故之间存在因果关系后立即提交报告，但不得迟于提供者或者，如适用部署者意识到严重事故之日起10天。
1e.必要时，为确保及时报告，提供者或部署者（如适用）可提交一份不完整的初次报告，然后再提交一份完整的报告。

1a. 在根据第1款报告严重事故后，提供者应毫不拖延地对严重事故和相关的人工智能系统进行必要的调查。调查应包括对事故的风险评估和纠正措施。在第一项所指的调查期间，提供者应与主管机关合作，并在相关情况下与有关通知机关合作，在向主管机关通报此类行动之前，不得进行任何涉及以可能影响随后对事故原因进行评估的方式改变有关人工智能系统的调查。
2. 在收到与第3条第44项c点所述严重事件有关的通知后，相关市场监督管理机关应通知第64条第3款所述国家公共机关或机构。委员会应制定专门指南，以促进遵守第1款规定的义务。该指南最迟应在本条例生效12个月后发布，并应定期评估。
2a. 市场监督管理机关应在收到第1款所述通知之日起7天内采取2019/1020号条例第19条规定的适当措施，并遵循2019/1020号条例规定的通知程序。
3. 对于附件三所述的高风险人工智能系统，如果其投放市场或投入使用的提供者受制于规定了与本条例同等报告义务的欧盟法律文书，则严重事故的通报应仅限于第3条第44项c点所述的情况。
3a. 对于属于2017/745号法规和2017/746号法规所涵盖的设备安全组件或设备本身的高风险人工智能系统，严重事故的通报应仅限于第3条第44项c点中提及的事故，并应向事故发生地成员国为此目的选择的国家主管机关通报。
3a. 国家主管机关应根据2019/1020号条例第20条的规定，立即向欧盟委员会通报任何严重事件，无论欧盟委员会是否已就此采取行动。

第3章
执法

第63条
联盟市场对人工智能系统的市场监督和控制

1. 2019/1020号条例适用于本条例所涵盖的人工智能系统。但是，为了有效执行本条例
(a) 凡提及2019/1020号条例的经济运营商，均应理解为包括本条例第2条第1款确定的所有运营商；
(b) 凡提及2019/1020 号条例规定的产品，均应理解为包括本条例范围内的所有人工智能系统。
2. 作为2019/1020号条例第34条第4款规定的报告义务的一部分，市场监督管理机关应每年向欧盟委员会和相关国家竞争管理机构报告在市场监督活动过程中发现的可能与适用欧盟竞争规则法有关的任何信息。它们还应当每年向欧盟委员会报告当年发生的使用违禁实践的情况以及所采取的措施。
3. 对于与附件二A节所列法律行为适用的产品有关的高风险人工智能系统，为本条例的目的，市场监督管理机关应是负责根据这些法律行为指定的市场监督活动的机构。在有正当理由的情况下，成员国可克减上段的规定，指定另一个有关机关作为市场监督管理机关，但须确保与负责执行附件二所列法律行为的有关部门市场监督管理机关进行协调。
3a. 本条例第65、66、67和68条所述程序不适用于与产品有关的人工智能系统，附件二A部分所列的法律行为适用于这些系统，如果这些法律行为已经规定了确保同等保护水平并具有相同目标的程序。在这种情况下，应适用这些部门的程

序。
3b. 在不影响2019/1020号条例第14条规定的市场监督管理机关的权力的情况下，为确保本条例的有效实施，市场监督管理机关可酌情远程行使2019/1020号条例第14条第4款d项和j项所述的权力。
4. 对于由受欧盟金融服务立法监管的金融机构投放市场、投入使用或使用的高风险人工智能系统，只要人工智能系统的投放市场、投入使用或使用与提供这些金融服务直接相关，则为本条例目的，市场监督管理机关应是根据该立法负责对这些机构进行金融监管的相关国家机关。
4a. 通过对上一分段的克减，在有正当理由的情况下，并在确保协调的前提下，成员国可为本条例的目的确定另一个相关机关作为市场监督管理机关。
根据2013/36/EU号指令对受监管信贷机构进行监管的国家市场监督管理机关，如果参与了根据1204/2013号理事会法规建立的单一监管机制（SSM），则应毫不迟延地向欧洲中央银行报告在其市场监管活动过程中发现的可能与欧洲中央银行根据该法规规定的审慎监管任务有关的任何信息。
5. 对于第1点所列的高风险人工智能系统，只要该系统用于执法目的和附件三第6、7和8点所列目的，成员国应为本条例之目的指定2016/679号条例或2016/680号指令规定的数据保护主管监督机构或根据2016/680号指令第1至44条规定的相同条件指定的任何其他机构为市场监督管理机关。市场监督活动不得以任何方式影响司法机关的独立性，也不得以其他方式干扰司法机关以司法身份开展的活动。
6. 如果联盟机构、机关和团体属于本条例的适用范围，欧洲数据保护监督员应作为其市场监督管理机关行事，但与以司法身份行事的法院有关的情况除外。
7. 成员国应促进根据本条例指定的市场监督管理机关与其他相关国家机关或机构之间的协调，这些机关或机构负责监督附件二所列欧盟统一立法或可能与附件三所述高风险人工智能系统相关的其他欧盟立法的实施。
7a. 市场监督管理机关和委员会应能够提议开展联合活动，包括由市场监督管理机关或市场监督管理机关与委员会联合开展的联合调查，其目的是促进合规、查明不合规情况、提高认识，并根据2019/1020号文件第9条，针对被发现在多个成员国构成严重风险的特定类别高风险人工智能系统提供与本条例有关的指导。人工智能办公室应为联合调查提供协调支持。
7a. 在不影响2019/1020号条例规定的权力的情况下，并在相关且仅限于履行其任务所必需的情况下，提供者应允许市场监督管理机关完全访问用于开发高风险人工智能系统的文件以及培训、验证和测试数据集，包括在适当且符合安全保障的情况下，通过应用程序编程接口（“API”）或其他相关技术手段和工具实现远程访问。
7b. 市场监督管理机关应根据合理的请求，并只有在满足以下累累进条件的情况下，方可获准查阅高风险人工智能系统的源代码：
(a) 为评估高风险人工智能系统是否符合第三编第2章的要求，有必要获取源代码，以及
(b) 基于提供者提供的数据和文件的测试/审计程序和核查已经用尽或者已证明不充分。
7c. 市场监督管理机关获得的任何信息和文件均应按照第70条规定的保密义务处理。

第63a条
通用人工智能系统的互助、市场监督和控制

1. 如果人工智能系统基于通用人工智能模型，且模型和系统由同一提供者开发，则人工智能办公室应有权监测和监督该人工智能系统遵守本条例义务的情况。为执行监测和监督任务，人工智能办公室应拥有2019/1020号条例所指的市场监督管理机关的所有权力。
2. 如果相关市场监督管理机关有充分理由认为，可由部署者直接用于至少一种根据本条例被归类为高风险的目的的通用人工智能系统不符合本条例规定的要求，则应与人工智能办公室合作，对合规情况进行评估，并相应地通知理事会和其他市场监督管理机关。
3. 当一个国家市场监督管理机关因无法获得与人工智能模型有关的某些信息而无法完成对高风险人工智能系统的调查时，尽管其已做出一切适当努力来获得这些信息，其仍可向人工智能办公室提出合理的请求，以便能够强制获得这些信息。在这种情况下，人工智能办公室应毫不拖延地向申请机关提供人工智能办公室认为与确定高风险人工智能系统是否不合规有关的任何信息，无论如何应在30 天内提供。国家市场主管机关应根据第70条的规定对所获得的信息保密。1020/2019号条例第6章规定的程序应类推适用。

第63b条
市场监督管理机关对真实情况下的测试进行监督

1. 市场监督管理机关应有权确保在真实世界条件下进行的检测符合本条例的规定。
2. 如果根据第54条在人工智能监管沙盒内对受监管的人工智能系统进行真实世界条件下的测试，市场监督管理机关应核查第54a条规定的遵守情况，作为其对人工智能监管沙盒的监管作用的一部分。这些机关可酌情允许提供者或潜在提供者在真实世界条件下进行测试，以克减第54a条第4款第f和g项规定的条件。
3. 如果潜在提供者、提供者或任何第三方告知市场监督管理机关发生了严重事故，或有其他理由认为第54a条和第54b条规定的条件未得到满足，市场监督管理机关可在其境内酌情做出以下任何决定：
(a) 中止或终止真实世界条件下的测试；
(b) 要求提供者或潜在提供者和使用者在真实世界条件下修改测试的任何方面。
4. 如果市场监督管理机关已做出本条第3款所述的决定，或已发出第54a条第4款第b项所指的反对意见，则该决定或反对意见应说明理由以及提供者或潜在提供者对该决定或反对意见提出质疑的方式和条件。
5. 在适用的情况下，如果市场监督管理机关做出了本条第3款所述的决定，则应将其理由通知按照测试计划对人工智能系统进行了测试的其他成员国的市场监督管理机关。

第64条
保护基本权利的机关的权力

3. 负责监督或强制执行与使用附件三所述高风险人工智能系统有关的欧盟法律规定的保护基本权利（包括不受歧视的权利）的义务的国家公共机关或机构，应有权要求并获取根据本条例以无障碍语言和格式创建或维护的任何文件，如果获取该文件是在其管辖范围内有效履行其职责所必需的。有关公共机关或机构应将任何此类要求通知有关成员国的市场监督管理机关。
4. 在本条例生效后三个月内，各成员国应确定第3款提及的公共机关或机构，并公布一份名单。各成员国应将该名单通报欧盟委员会和所有其他成员国，并不断更新该名单。
5. 如果第3款提及的文件不足以确定是否发生了违反旨在保护基本权利的欧盟法律规定的义务的情况，第3款提及的公共机关或机构可向市场监督管理机关提出合理请求，通过技术手段组织对高风险人工智能系统的测试。市场监督管理机关应在收到请求后的合理时间内，在提出请求的公共机关或机构的密切参与下组织测试。
6. 第3款提及的国家公共机关或机构根据本条规定获得的任何信息和文件均应按照第70条规定的保密义务处理。

第65条
处理在国家层面构成风险的人工智能系统的程序

1. 就对人的健康或安全或基本权利的风险而言，具有风险的人工智能系统应被理解为具有2019/1020号条例第3条第19点所定义的风险的产品。
2. 如果成员国的市场监督管理机关有充分理由认为人工智能系统存在第1款所述的风险，则应对相关人工智能系统遵守本条例规定的所有要求和义务的情况进行评估。应特别关注对弱势群体构成风险的人工智能系统，见第5 条。当发现基本权利面临风险时，市场监督管理机关还应通知第64条第3款所述的相关国家公共机关或机构，并与之充分合作。相关经营者应与市场监督管理机关和其他国家公共机关或机构进行必要的合作。
在评估过程中，如果市场监督管理机关发现人工智能系统不符合本条例规定的要求和义务，应在没有无故拖延的情况下，要求相关经营者采取一切适当的纠正措施，使人工智能系统符合要求，从市场上撤回人工智能系统，或在其规定的期限内召回人工智能系统，无论如何不得迟于15个工作日，或根据适用的相关欧盟协调法的规定。
市场监督管理机关应相应通知相关的通知机关。2019/1020号条例第18条应适用于第二款所述措施。
3. 如果市场监督管理机关认为不遵守规定的情况不限于本国境内，则应将评估结果和要求经营者采取的行动通知欧盟委员会和其他成员国，不得无故拖延。
5. 如果人工智能系统的经营者在第2款所述期限内没有采取适当的纠正行动，市场监督管理机关应采取一切适当的临时措施，禁止或限制该人工智能系统在其本国市场上销售或投入使用，从该市场上撤回该产品或独立的人工智能系统，或将其召回。该机关应毫不拖延地将这些措施通知欧盟委员会和其他成员国。
6. 第5款所述通知应包括所有现有细节，特别是识别不符合要求的人工智能系统所需的信息、人工智能系统的来源和供应链、所指控的不符合要求行为的性质和所涉及的风险、所采取的国家措施的性质和持续时间以及相关经营者提出的论据。尤其是，市场监督管理机关应说明不合规行为是否是由以下一个或多个

原因造成的：
(a) 不遵守第5条所述禁止人工智能实践的规定；
(a) 高风险人工智能系统未能达到第三编第2章规定的要求；
(ba) 不遵守第52条的规定；
7. 除启动程序的成员国的市场监督管理机关外，其他成员国的市场监督管理机关应毫不拖延地向委员会和其他成员国通报所采取的任何措施和它们所掌握的与有关人工智能系统不符合要求有关的任何补充信息，并在不同意所通报的国家措施的情况下，通报它们的反对意见。
8. 如果在收到第5款所述通知后三个月内，一个成员国的市场监督管理机关或欧盟委员会均未对另一个成员国的市场监督管理机关采取的临时措施提出异议，则该措施应被视为合理。这不影响相关经营者根据2019/1020号条例第18条享有的程序权利。在不遵守第5条所述禁止人工智能实践的情况下，本款第一句所述的期限应缩短至30天。
9. 所有成员国的市场监督管理机关都应确保对有关产品或人工智能系统采取适当的限制性措施，如没有无故拖延地将产品或人工智能系统撤出其市场。

第65a条
处理被提供者归类为适用附件三的非高风险人工智能系统的程序

1. 如果市场监督管理机关有充分理由认为，提供者在适用附件三时归类为非高风险的人工智能系统属于高风险系统，则该市场监督管理机关应根据附件三和欧盟委员会准则规定的条件，对有关人工智能系统是否归类为高风险人工智能系统进行评估。
2. 如果在评估过程中，市场监督管理机关发现有关的人工智能系统具有高风险，其应毫不拖延地要求有关提供者采取一切必要行动，使人工智能系统符合本条例规定的要求和义务，并在它可能规定的期限内采取适当的纠正行动。
3. 如果市场监督管理机关认为有关人工智能系统的使用不限于其本国领土，则应将评估结果和要求提供者采取的行动通知委员会和其他成员国，不得无故拖延。
4. 提供者应确保采取一切必要行动，使人工智能系统符合本条例规定的要求和义务。如果有关人工智能系统的提供者没有在第2款提及的期限内使人工智能系统符合本条例的要求和义务，则应根据第71条对提供者处以罚款。
5. 提供者应确保对其在全联盟市场上销售的所有相关人工智能系统采取一切适当的纠正措施。
6. 如果有关人工智能系统的提供者在第2款所述期限内没有采取适当的纠正措施，则适用第65条第5至第9款的规定。
7. 如果在根据第1款进行评估的过程中，市场监督管理机关确定人工智能系统被提供者错误地归类为非高风险系统，以规避适用第三编第2章的要求，则应根据第71条对提供者处以罚款。
8. 在行使其监督本条适用情况的权力时，根据2019/1020号条例第11条，市场监督管理机关可进行适当的检查，特别是考虑到第60条所述欧盟数据库中存储的信息。

第66条

联盟保障程序

1. 在收到第65条第5款所述通知后3个月内，或在不遵守第5条所述禁止人工智能实践的情况下的30天内，如果一个成员国的市场监督管理机关对另一个市场监督管理机关采取的措施提出异议，或者如果委员会认为该措施违反欧盟法律，委员会应在没有无故拖延的情况下，与相关成员国的市场监督管理机关和一个或多个经营者进行协商，并对该国家措施进行评估。根据评估结果，委员会应在第65条第5款所述通知发出后的六个月内，或在不遵守第5条所述禁止人工智能实践的情况下的60天内，决定该国家措施是否合理，并将该决定通知相关成员国的市场监督管理机关。委员会还应将此决定通知所有其他市场监督管理机关。
2. 如果委员会认为有关成员国采取的措施是合理的，所有成员国应确保对有关的人工智能系统采取适当的限制性措施，如从其市场上撤出人工智能系统，不得无故拖延，并应将有关情况通知委员会。如果委员会认为国家措施不合理，有关成员国应撤销该措施，并向委员会通报。

第66a条
联合调查

如果国家监管机关有理由怀疑本条例高风险人工智能系统或基础模型的提供者或部署者的侵权行为构成具有联盟层面的广泛侵权行为，或影响或可能影响一个以上成员国的至少4500万个人，则该国家监管机关应通知人工智能办公室，并可要求发生侵权行为的成员国的国家监管机关启动联合调查。人工智能办公室应为联合调查提供中央协调。调查权仍属于国家监督机构。
3. 如果国家措施被认为是合理的，并且人工智能系统的不合规性归咎于本条例第40和41条中提及的统一标准或共同规格的缺陷，则欧盟委员会应适用1025/2012号条例第11条规定的程序。

第67条
存在风险的合规人工智能系统

1. 如果成员国的市场监督管理机关在根据第65条进行评估，并与第64条第3款提及的相关国家公共机关协商后，发现虽然高风险人工智能系统符合本条例的规定，但对人的健康或安全、基本权利或公共利益保护的其他方面构成风险，则应要求相关经营者采取一切适当措施，确保有关人工智能系统在投放市场或投入使用时，在其规定的期限内不再构成风险，不得无故拖延。
2. 提供者或其他相关运营商应确保在第1款所述成员国市场监督管理机关规定的时限内，对其在全联盟市场上提供的所有相关人工智能系统采取纠正行动。
2a. 如果提供者或其他相关经营者未能采取第2款所述的纠正措施，而且人工智能系统继续存在第1款所述的风险，国家监管机关可要求相关经营者在与风险性质成比例的合理期限内将人工智能系统撤出市场或召回。
3. 成员国应立即通知委员会和其他成员国。这些信息应包括所有可获得的详细资料，特别是识别有关人工智能系统的必要数据、人工智能系统的来源和供应链、所涉风险的性质以及所采取的国家措施的性质和持续时间。

4. 委员会应及时与有关成员国和相关经营者进行磋商，并对各国采取的措施进行评估。根据评估结果，委员会应决定该措施是否合理，并在必要时提出适当的措施。
5. 委员会应立即将其决定通知有关成员国和相关运营商。委员会还应将其决定通知所有其他成员国。
5a. 委员会应通过指南，帮助各国主管机关发现并在必要时纠正其他人工智能系统中出现的类似问题。

第68条
形式违规

1. 如果成员国的市场监督管理机关得出以下结论之一，则应要求相关提供者在其可能规定的期限内停止有关违规行为：
(a) 加贴CE标志的行为违反了第49条的规定；
(b) 未加贴CE标志；
(ea) 尚未在欧盟数据库中登记；
(eb) 在适用的情况下，未指定授权代表。
(ec) 不具备技术文件
2. 如果第1款所述违规行为持续存在，有关成员国的市场监督管理机关应采取适当和成比例的措施，限制或禁止高风险人工智能系统在市场上销售，或确保毫不拖延地从市场上召回或撤回该系统。

第68a条
欧盟人工智能领域的人工智能测试支持结构

1. 欧盟委员会应指定一个或多个欧盟人工智能测试支持结构，在人工智能领域执行1020/2019号条例第21条第6款所列的任务。
2. 在不影响第1款所述任务的前提下，欧盟人工智能检测支持结构还应根据欧洲人工智能委员会、欧盟委员会或市场监督管理机关的要求，提供独立的技术或科学建议。

第3b章（新增）
救济措施

第68a条
向市场监督管理机关投诉的权利

1. 在不影响其他行政或司法补救措施的情况下，任何自然人或法人如有理由认为本条例的规定受到违反，均可向相关市场监督管理机关提出申诉。
根据2019/1020号法规，在开展市场监督活动时应考虑投诉，并按照市场监督管理机关制定的专门程序进行处理。

第1章
对通用人工智能模型提供者的监督、调查、执法和监测

第A条
执行通用人工智能模型提供者的义务

1.委员会拥有监督和执行[通用人工智能模型]章/标题的专属权力，同时考虑第H条规定的程序保障。委员会应委托欧洲人工智能办公室执行这些任务，但不得损害委员会的组织权力以及成员国和联盟之间根据条约进行的权限划分。
2.在不影响第63a条第3款的情况下，市场监督管理机关可请求欧盟委员会行使本章规定的权力，只要这样做对协助其完成本条例规定的任务是必要和成比例的。

第B条
监测行动

为执行本章规定的任务，人工智能办公室可采取必要行动，监测通用人工智能模型提供者对本条例的有效执行和遵守情况，包括对经批准的行为守则的遵守情况。
2.下游提供者有权就违反本条例的行为提出申诉。投诉应充分说明理由，并至少说明：
(a) 有关通用人工智能模型提供者的联络点；
(b) 描述相关事实、本条例的相关规定以及下游提供者认为相关通用人工智能模型的提供者违反本条例的原因；
(c) 发出请求的下游提供者认为相关的任何其他信息，包括酌情主动收集的信息。

第C条
科学小组对系统性风险的警报

1.当科学小组有理由怀疑以下情况时，可向人工智能办公室发出有保留的警报
(a) 通用人工智能模型在联盟层面构成具体的可识别风险；或
(b) 通用人工智能模型符合具有系统风险的通用人工智能模型的分类一条所指的要求。
2.在接到这种有条件的警报后，通过人工智能办公室，并在通知欧洲人工智能委员会后，委员会可行使本章规定的权力，对问题进行评估。人工智能办公室应将根据第D-H条采取的任何措施通知委员会。
3.有保留的警报应充分说明理由并至少表明：
(a) 通用人工智能模型提供者与有关系统风险的联系点；
(b) 说明科学小组怀疑的相关事实和理由；
(c) 科学小组认为相关的任何其他信息，包括酌情主动收集的信息。

第D条
要求提供文件和信息的权力

1.委员会可要求相关通用人工智能模型的提供者提供其根据通用人工智能模型

提供者的义务和具有系统性风险的通用人工智能模型提供者的义务的相应条款起草的文件，或为评估该提供者遵守本条例的情况所需的任何补充信息。
2.在发出提供信息的请求之前，人工智能办公室可与通用人工智能模型的提供者开展有组织的对话。
3.根据科学小组提出的理由充分的请求，委员会可向通用人工智能模型的提供者发出提供信息的请求，条件是根据科学小组条第2款的规定，获取信息对于完成科学小组的任务是必要的和成比例的。
4.信息申请应说明申请的法律依据和目的，具体说明需要哪些信息，并规定提供信息的期限，以及第4条规定的对提供不正确、不完整或误导性信息的罚款。
5.相关通用人工智能模型的提供者或其代表，如果是法人、公司或企业，或如果其不具备法人资格，则由法律或其章程授权加以代表的人，应代表相关通用人工智能模型的提供者提供所要求的信息。经正式授权的律师可代表其委托人提供信息。如果提供的信息不完整、不正确或有误导性，委托人应承担全部责任。

第E条
进行评估的权力

1.人工智能办公室在咨询欧洲人工智能委员会后，可对有关的通用人工智能模型进行评估
(a) 在根据第D条收集的信息不充分的情况下，评估提供者遵守本条例规定的义务的情况；或
(b) 在联盟层面调查具有系统性风险的通用人工智能模型的系统性风险，特别是在科学小组根据关于通用人工智能模型和具有系统性风险的通用人工智能模型提供者的义务的条款的第3款第c点提出有保留的报告之后。
2.委员会可决定任命独立专家代表其进行评估，包括根据第58b条从科学小组中任命独立专家。为此任务任命的所有独立专家均应符合第58b条第2款规定的标准。
3.为第1款之目的，委员会可要求通过应用程序接口（API）或其他适当的技术手段和工具，包括通过源代码，获取有关的通用人工智能模型。
4.查阅申请应说明申请的法律依据、目的和理由，并规定提供查阅的期限，以及第4条规定的对不提供查阅的罚款。
5.有关通用人工智能模型的提供者，如果是法人、公司或企业，或者不具备法人资格，则应由法律或其章程授权加以代表的人代表有关通用人工智能模型的提供者提供所要求的访问。
6.评估的方式和条件，包括独立专家的参与方式和遴选独立专家的程序，应在实施法案中加以规定。这些实施法案应根据第xx条第x款提及的审查程序通过。
7.在要求查阅有关的通用人工智能模型之前，人工智能办公室可与通用人工智能模型的提供者开展有组织的对话，以收集更多关于模型内部测试、防止系统性风险的内部保障措施以及提供者为减少此类风险而采取的其他内部程序和措施的信息。

第F条
要求采取措施的权力

1. 在必要和适当的情况下，委员会可要求提供者
(a) 采取适当措施，在相应的编和章中规定通用人工智能模型提供者的义务；
(b) 要求提供者实施缓解措施，条件是根据规定评估权的相应条款进行的评估引起了对联盟层面系统性风险的严重且确凿的担忧；
(c) 限制在市场上销售、撤回或召回该模型产品。
2. 在要求采取某项措施之前，人工智能办公室可与通用人工智能模型的提供者开展有组织的对话。
3. 如果在第2款规定的结构性对话期间，具有系统性风险的通用人工智能模型的提供者承诺采取缓解措施，以应对联盟层面的系统性风险，则委员会可通过决定使这些承诺具有约束力，并宣布没有进一步采取行动的理由。

第H条
通用人工智能模型经济运营商的程序性权利

2019/1020号条例第18条通过类推而适用于通用人工智能模型的提供者，但不影响本条例中规定的更具体的程序性权利。

第68c条
获得个体决策的解释的权利

1. 任何受部署者根据附件三所列高风险人工智能系统（第2点所列系统除外）的输出结果所做决定影响的人，如果认为该决定对其健康、安全和基本权利产生了不利影响，并产生了法律效力或类似的重大影响，应有权要求部署者就人工智能系统在决策程序中的作用和所做决定的主要内容做出明确而有意义的解释。
2. 第1款不适用于根据联盟法律或国家法律对第1款规定的义务有例外或限制的人工智能系统的使用。
3. 本条仅适用于第1款所述权利尚未在联盟法律中做出规定的情况。

第68d条
修订2020/1828号指令

在欧洲议会和欧盟理事会指令2020/1828的附件一[30]中，增加以下内容：
“(67a) 关于欧洲议会和欧盟理事会制定有关人工智能的统一规则xxxx/xx号条例（《人工智能法》）以及修订若干联盟立法的建议（官方公报……）。“

第68e条
违规行为的举报和对举报人的保护

欧洲议会和欧盟理事会2019/1937号指令应适用于对本条例违规行为的举报和对违规行为举报人的保护。

[30] 2020 年 11 月 25 日欧洲议会和理事会关于保护消费者集体利益的代表行动并废除 2009/22/EC 号指令的 2020/1828 号指令（官方公报，L 409，2020 年 12 月 4 日，第 1 页）。

第9章
行为守则

第69条
自愿执行特定要求的行为守则

1. 人工智能办公室和成员国应鼓励和促进制定行为守则，包括相关的管理机制，以促进除高风险人工智能系统外的人工智能系统自愿适用本条例第三篇第二章中的部分或全部要求，同时考虑到允许适用这些要求的现有技术解决方案和行业最佳实践。
2. 人工智能办公室和成员国应促进制定行为守则，根据明确的目标和衡量这些目标实现情况的关键绩效指标，包括但不限于以下内容，对所有人工智能系统自愿适用具体要求，包括由部署者自愿适用这些要求：
(a) 欧洲可信人工智能伦理准则中所预见的适用的要件；
(b) 评估并最大限度地减少人工智能系统的影响，包括节能编程和高效设计、训练和使用人工智能的技术；
(c) 促进对人工智能素养，特别是对从事人工智能开发、操作和使用的人员的素养提升；
(d) 促进人工智能系统设计的包容性和多样性，包括建立包容性和多样性的开发团队，促进利益相关方参与这一进程；
(e) 评估和预防人工智能系统对弱势人员或群体的负面影响，包括对残疾人的无障碍性以及对性别平等的负面影响。
3. 行为守则可由人工智能系统的个别提供者或部署者或代表他们的组织或由两者共同拟订，包括在部署者和任何有关利益相关方及其代表组织，包括公民社会组织和学术界，的参与下拟订。考虑到相关系统的预期目的的相似性，行为守则可涵盖一个或多个人工智能系统。
4. 在鼓励和促进制定行为守则时，人工智能办公室和成员国应考虑到包括初创企业在内的小微型企业的具体利益和需要。

第X编
保密和处罚

第70条
保密性

1. 欧盟委员会、市场监督管理机关和通知机关以及参与实施本条例的任何其他自然人或法人，应根据欧盟或国家法律，尊重在执行其任务和活动过程中获得的信息和数据的保密性，特别是保护：
(a) 知识产权，以及自然人或法人的商业机密信息或商业秘密，包括源代码，但关于保护未披露的专有技术和商业信息（商业秘密）免遭非法获取、使用和披露的2016/943号指令第5条所述情况除外。
(b) 本条例的有效实施，特别是为了检查、调查或审计的目的；
(ba) 公共和国家安全利益；

(c) 刑事或行政诉讼的整全性。
(da) 根据联盟或国家法律分类的信息的整全性。
(db) 1a. 根据第1款适用本条例的有关机关只应要求提供对评估人工智能系统所构成的风险以及根据本条例和2019/1020号条例行使其权力严格必要的数据。他们应采取充分有效的网络安全措施，以保护所获取信息和数据的安全性和保密性，并应根据适用的国家或欧洲立法，在不再需要用于所请求的目的时，立即删除所收集的数据。
2. 在不影响第1款和第1a款的情况下，当执法、边境管制、移民或庇护机关 使用附件三第1、6和7点所述高风险人工智能系统时，在国家主管机关之间以及国家主管机关与委员会之间在保密基础上交流的信息，如其披露将危及公共和国家安全利益，则未经事先与提供信息的国家主管机关和部署者协商，不得披露。这种信息交流不应包括与执法、边境管制、移民或庇护机关的活动有关的敏感业务数据。
当执法、移民或庇护机关是附件三第1、6和7点所述高风险人工智能系统的提供者时，附件四所述技术文件应留存在这些机关的办公场所内。这些机关应确保第63条第5款和第6款所指的市场监督管理机关，视适用情况而定，可应要求立即查阅这些文件或获得其副本。只有持有适当级别安全许可的市场监督管理机关工作人员方可查阅该文件或其任何副本。
3. 第1款和第2款不影响委员会、成员国及其有关机关以及通知机关在交流信息和传播警示方面的权利和义务，包括在跨境合作中的权利和义务，也不影响有关各方根据成员国刑法提供信息的义务。
4. 必要时，委员会和成员国可根据国际和贸易协定的相关规定，与已缔结双边或多边保密安排、保证充分保密的第三国监管机关交换机密信息。

第71条
罚则

1. 根据本条例规定的条款和条件，成员国应制定适用于经营者违反本条例行为的处罚规则和其他执行措施，其中也可包括警告和非罚款措施，并应采取一切必要措施，确保这些规则和措施得到适当和有效的执行，同时考虑到委员会根据第82b条发布的指南。规定的处罚应有效、适度并具有阻遏性。处罚应考虑包括初创企业在内的小微型企业的利益及其经济可行性。
2. 成员国应毫不迟延地将各自的规则和措施通知委员会，最迟在这些规则和措施生效之日通知委员会，并应毫不迟延地将随后对其产生影响的任何修正通知委员会。
3. 不遵守第5条所述禁止人工智能行为的规定，将被处以最高3500万欧元的行政罚款，如果违规者是公司，则最高罚款额为其上一财政年度全球年营业总额的7%，以较高者为准：
4. 除第5条规定外，人工智能系统如不遵守以下任何一条与运营者或通知机构有关的规定，将被处以最高1500万欧元的行政罚款，如果违法者是公司，则处以最高相当于其上一财政年度全球年营业总额3%的罚款，以数额较高者为准：
(a) 第4b和第4c条规定的提供者义务；
(b) 第16条规定的提供者义务；
(c) 第23a条规定的某些其他人的义务；

(d) 第25条规定的授权代表的义务；
(e) 第26条规定的进口者的义务；
(f) 第27条规定的分销者的义务；
(g) 第29条第1款至第6a款规定的用户义务；
(h) 根据第33、第34条第1款、第34第3款、第34第4款、第34a条通知机构的要求和义务；
(i) 第52条规定的提供者和使用者的透明度义务。
4a. 如果是小微型企业，包括新成立的企业，罚款额最高可达其上一财政年度全球年营业额的2%。
5. 应要求向通知机关和国家主管机关提供不正确、不完整或误导性信息的，应处以最高7500000欧元的行政罚款；如果违法者是公司，则处以最高相当于其上一财政年度全球年营业总额1%的行政罚款，以数额较高者为准。
5a. 对于小微型企业，包括新成立的企业，本条所指的每项罚款应达到第3、第4和第5款所指的百分比或金额，以两者中较低者为准。
6. 在决定是否处以行政罚款以及每起个案的行政罚款数额时，应考虑具体情况的所有相关因素，并酌情考虑以下因素：
(a) 侵权行为及其后果的性质、严重程度和持续时间，同时考虑到人工智能系统的目 的，并酌情考虑受影响者的人数及其所受损害的程度；
(aa) 侵权行为的故意或过失性质；
(ab) 经营者为纠正侵权行为和减轻侵权行为可能造成的不利影响而采取的任何行动；
(b) 一个或多个成员国的其他市场监督管理机关是否已对同一经营者的同一违法行为处以行政罚款；
(ba) 如果同一经营者因违反其他联盟或国家法律而被其他机关处以行政罚款，而这些违法行为是由构成违反本法案相关行为的同一活动或不作为造成的；
(c) 侵权经营者的规模、年营业额和市场份额；
(ca) 适用于案件情节的任何其他加重或减轻处罚的因素，如直接或间接从侵权行为中获得的经济利益或避免的损失。
(ca) 为纠正侵权行为和减轻侵权行为可能造成的负面影响而与国家主管机关合作的程度；
(cb) 考虑到经营者采取的技术和组织措施，经营者责任的程度
(cc) 遵守经批准的行为守则或经批准的认证机制；
(ce) 国家主管机关了解侵权行为的方式，特别是经营者是否通知了侵权行为，如果是，通知的程度如何；
(cf) 侵权行为的故意或过失性质
(cg) 经营者为减轻受影响者所遭受的损害而采取的任何行动；
7. 各成员国应制定规则，规定可在多大程度上对在其境内设立的公共机关和机构处以行政罚款。
8. 根据成员国的法律制度，行政罚款规则的适用方式可以是由主管国家法院或在这些成员国适用的其他机关处以罚款。此类规则在这些成员国的适用具有同等效力。
8a. 市场监督管理机关行使本条规定的权力时，应遵守欧盟和成员国法律规定的适当程序保障，包括有效的司法救济和正当程序。
8b. 成员国应每年向委员会报告其在该年度内根据本条规定所开出的行政罚单，

以及任何相关的诉讼或司法程序。

第72条
对联盟机构、机关和团体的行政罚款

1.欧洲数据保护监督员可对本条例范围内的联盟机构、机关和团体处以行政罚款。在决定是否处以行政罚款以及决定每个个案的行政罚款金额时，应考虑具体情况的所有相关因素，并适当考虑以下因素：
(a) 侵权行为及其后果的性质、严重程度和持续时间，同时考虑到有关人工智能系统的目的、受影响者的人数及其所受损害的程度，以及任何相关的先前侵权行为；
(aa) 联盟机构、机关或团体的责任程度，同时考虑到其实施的技术和组织措施；
(ab) 联盟机构、机关或团体为减轻受影响者所遭受的损害而采取的任何行动；
(b) 与欧洲数据保护监督员合作的程度，以纠正侵权行为和减轻侵权行为可能造成的不利影响，包括遵守欧洲数据保护监督员以前就同一主题事项对有关联盟机构或机关或团体下令采取的任何措施；
(c) 联盟机构、机关或团体以前的任何类似违规行为；
(ca) 欧洲数据保护监督员了解侵权行为的方式，特别是欧盟机构或组织是否通知了侵权行为，以及通知的程度；
(cb) 机构的年度预算。
2.不遵守第5条所述禁止人工智能行为的规定，将被处以最高1500000欧元的行政罚款。
3. 除第5条规定的要求或义务外，对不遵守本条例规定的任何要求或义务的人工智能系统处以最高75万欧元的行政罚款。
4.在根据本条做出决定之前，欧洲数据保护监督员应给予作为欧洲数据保护监督员诉讼主体的联盟机构、机关或团体就可能的侵权事项陈述意见的机会。欧洲数据保护监督员应仅根据有关各方能够发表意见的内容和情况做出决定。投诉人，如有，应密切参与诉讼程序。
5.在诉讼过程中，有关各方的辩护权应得到充分尊重。在不违背个人或企业保护其个人数据或商业秘密的合法利益的情况下，其有权查阅欧洲数据保护监督员的档案。
6.根据本条规定征收的罚款应纳入联盟总预算。罚款不得影响被罚款的联盟机构、团体或机关的有效运作。
6a. 欧洲数据保护监督员应每年向欧盟委员会通报其根据本条款实施的行政罚款以及任何诉讼或司法程序；

第72a条
对通用人工智能模型提供者的罚款

1.委员会可对通用人工智能模型提供者处以不超过其上一财政年度全球总营业额3%或1500万欧元的罚款，以金额较高者为准。罚款应在本条例相关条款生效一年后加以惩处，以便在委员会发现提供者故意或疏忽时，让提供者有足够的时间进行调整：

(a) 违反本条例的有关规定；
(b) 未能遵守根据要求提供文件和信息的权力的条款提出的提供文件或信息的要求，或提供不正确、不完整或有误导性的信息；
(b) 未遵守根据要求采取措施的权力的条款要求采取的措施；
(c) 未向委员会提供通用人工智能模型或具有系统性风险的通用人工智能模型的使用，以便其根据开展评估的权力进行评估。
在确定罚款或定期罚金的数额时，应考虑违法行为的性质、严重程度和持续时间，并适当考虑比例原则和适当原则。委员会还应考虑根据第F条第3款条做出的承诺或根据第C条第2款在相关行为守则中做出的承诺。
2. 在根据本条第1款通过决定之前，委员会应将其初步结论通知通用人工智能模型或具有系统风险的通用人工智能模型的提供者，并给予陈述意见的机会。
2a. 根据本条规定处以的罚款应适度、有效并具备阻遏性。
2b. 有关罚款的信息也应酌情通报欧洲人工智能委员会。
3. 欧盟法院拥有不受限制的管辖权，可审查委员会确定罚款数额的决定。法院可取消、减少或增加罚款。
4. 委员会应就根据第1款可能通过的决定的程序方式和实际安排通过实施法案。这些实施法案应根据第xx条第x款提及的审查程序通过。

第十一编
授权和委员会程序

第73条
行使授权

1. 根据本条规定的条件，委员会有权通过授权法案。
2. 第4条、第7条第1款、第11条第3款、第43条第5款和第6款以及第48条第5款提及的通过授权法案的权力授予委员会，自本条例生效之日起为期五年。委员会应在五年期结束前的九个月内起草一份有关授权的报告。除非欧洲议会或欧盟理事会在每一期限结束前三个月内反对延长，否则授权期限应默许延长至相同期限。
3. 第7条第1款、第7条第3款、第11条第3款、第43条第5和6款以及第48条第5款提及的授权可随时由欧洲议会或理事会撤销。撤销决定应终止该决定中规定的授权。撤销决定在《欧盟官方公报》上公布的次日或其后规定的日期生效。该决定不影响任何已生效的授权法案的有效性。
4. 欧盟委一旦通过授权法案，应同时通知欧洲议会和欧盟理事会。
5. 根据第7条第1款、第7条第3款、第11条第3款、第43条第5和6款以及第48条第5款通过的任何授权法案，只有在欧洲议会或欧盟理事会在向欧洲议会和欧盟理事会发出该法案通知后三个月内未表示反对，或欧洲议会和欧盟理事会在该期限届满前均已通知欧盟委员会它们不反对的情况下，方可生效。根据欧洲议会或理事会的倡议，该期限可延长三个月。

第74条
委员会程序

1.欧盟委员会应由一个委员会协助工作。该委员会应为182/2011号条例所指的委员会。
2. 在提及本款时，应适用182/2011号条例第5条。

第十二编
终则

第75条
修订300/2008号条例

在300/2008号条例第4条第3款中，增加以下分段：
“在采取和欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例[31]意义上的人工智能系统有关的安全设备的技术规格和批准及使用程序相关的详细措施时，应考虑到该条例第二编第3章中规定的要求。”

第76条
修订167/2013号条例

在167/2013号条例第17条第5款中，增加以下分段：
“在根据第一分段通过根据欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例[32]，属于安全组件的人工智能系统的授权法案时，应考虑到该条例第三编第2章规定的要求。”

第77条
修订168/2013号条例

在168/2013号条例第22条第5款中，增加以下分段：
“在根据第一分段通过关于欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例意义上的安全组件的人工智能系统的授权法案时[33]，应考虑到该条例第三编第2章规定的要求。”

第78条
修订2014/90/EU号指令

在2014/90/EU号指令第8条中，增加以下款：
“4.对于属于欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例[34]所指安全组件的人工智能系统，委员会在根据第1款开展活动以及根据第2款和第3款通过技术规范和测试标准时，应考虑到该条例第三编第2章规定的要求。”

第79条

[31] [有关人工智能的]YYY/XX号条例（官方公报……）。
[32] [有关人工智能的]YYY/XX 号条例（官方公报……）。
[33] [有关人工智能的]YYY/XX 号条例（官方公报……）。
[34] [有关人工智能的]YYY/XX 号条例（官方公报……）。

修订2016/797号指令

在2016/797号指令第5条中，增加以下款：
“12.在根据第1款通过涉及欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例[35]所指安全组件的人工智能系统的授权法案和根据第11款通过实施法案时，应考虑到该条例第三编第2章中规定的要求。

第80条
修订2018/858号条例

在2018/858号条例第5条中，增加以下款：
“4.在根据第3款通过关于欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例意义上的安全组件的人工智能系统的授权法案时[36]，应考虑到该条例第三编第2章规定的要求。”

第81条
修订2018/1139号条例

2018/1139号条例修订如下：
1. 在第17 条中，增加以下款
“3.在不影响第2款的情况下，在根据第1款通过有关属于欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例[37]所指安全组件的人工智能系统的实施法案时，应考虑到该条例第三编第2章中规定的要求。”
2. 在第19条中，增加以下款
“4.在根据第1款和第2款通过有关属于欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例意义上的安全组件的人工智能系统的授权法案时，应考虑到该条例第三编第2章规定的要求。”
3. 在第43条中，增加以下款
“4.在根据第1款通过有关属于[关于人工智能的]条例(欧盟)YYY/XX意义上的安全组件的人工智能系统的实施法案时，应考虑到该条例第三编第2章中规定的要求。”
4. 在第47条中，增加以下款
“3.在根据第1款和第2款通过有关属于[关于人工智能的]条例(欧盟)YYY/XX意义上的安全组件的人工智能系统的实施法案时，应考虑到该条例第三编第2章中规定的要求。”
5. 在第57条中，增加以下款
“在通过有关属于[关于人工智能的]条例(欧盟)YYY/XX意义上的安全组件的人工智能系统的实施法案时，应考虑到该条例第三编第2章中规定的要求。”
6. 在第58条中，增加以下款
“3.在根据第1款和第2款通过有关属于[关于人工智能的]条例(欧盟)YYY/XX意义上的安全组件的人工智能系统的实施法案时，应考虑到该条例第三编第2章中

[35] [有关人工智能的]YYY/XX 号条例（官方公报……）。
[36] [有关人工智能的]YYY/XX 号条例（官方公报……）。
[37] 欧洲议会和欧盟理事会[关于人工智能的]YYY/XX 号条例

规定的要求。”

第82条
修订2019/2144号条例

在2019/2144号条例第11条中，增加以下款：
"3.在根据第2款通过有关属于欧洲议会和欧盟理事会[关于人工智能的]YYY/XX号条例[38]所指安全组件的人工智能系统的实施法案时，应考虑到该条例第三编第2章中规定的要求。

第82a条
委员会关于实施本条例的指南

1.委员会应就本条例的具体实施制定指南，特别是：
(a) 第8-15条和第28条所述要求和义务的适用；
(b) 第5条所述的禁止行为；
(c) 有关实质性修改规定的实际执行情况；
(d) 第52条规定的透明度义务的实际执行情况；
(e) 本条例与本条例附件二中提及的立法以及其他相关欧盟法律之间关系的详细信息，包括执行过程中的一致性；
(f) 适用第3条第1款中关于人工智能系统的定义。
在发布此类指南时，欧盟委应特别关注包括初创企业在内的小微型企业、地方公共机关以及最有可能受本条例影响的部门的需求。
第一款提到的指南应适当考虑人工智能方面的先进技术水平，以及第40和第41条中提到的相关统一标准和共同规格，或根据欧盟协调法规定的统一标准或技术规格。
2.委员会应成员国或人工智能办公室的要求，或主动在其认为必要时更新已通过的指南。

第83条
已投放市场或投入使用的人工智能系统

1.在不影响第85条第3款第-aa项所述第5条的适用的情况下，属于附件九所列法案所建立的大型信息技术系统组成部分的、在第85条第2款所述本条例适用日期后12个月前已投放市场或投入使用的人工智能系统，应在2030年底前符合本条例的规定。
在对附件九所列法案所建立的每个大型信息技术系统进行评估时，应考虑到本条例规定的要求，这些评估应根据相关法案的规定进行，并在这些法案被取代或修订时进行。
2.在不影响第85条第3款第-aa项所述第5条的适用的情况下，本条例应适用于在第85条第2款所述本条例的适用日期之前已投放市场或投入使用的高风险人工智能系统，但第1款所述系统除外，的运营商，但仅限于自该日期起这些系统的设

[38] 欧洲议会和欧盟理事会[关于人工智能的]YYY/XX 号条例

计发生重大变化的情况。对于拟由公共机关使用的高风险人工智能系统，此类系统的提供者和部署者应在本条例生效之日起四年后采取必要步骤遵守本条例的要求。
3. 在第85条第3款第a项所述本条例的适用日期之前已投放市场的通用人工智能模型的提供者应采取必要步骤，以便在第85条第3款第a项所述本条例的适用日期之后两年内遵守本条例规定的义务。

第84条
评估和审查

1. 欧盟委员会应在本条例生效后每年评估一次附件三清单，即第5条所禁止的人工智能实践清单是否需要修订，直至授权期结束。委员会应将评估结果提交欧洲议会和理事会。
2. 在第85条第2款所述的本条例实施之日起两年内，以及此后每四年，欧盟委员会应评估并向欧洲议会和理事会报告是否有必要对以下内容进行修订：
- 扩大附件三中现有领域或增加新领域的必要性，
- 第52条中需要额外透明度措施的人工智能系统列表
- 监督和治理系统的有效性

2a. 在第85条第3款所述的本条例实施之日起三年内，以及此后每四年，欧盟委员会应向欧洲议会和理事会提交一份关于本条例评估和审查的报告。该报告应包括对执法结构的评估，以及是否有必要设立一个联盟机构来解决已发现的不足之处。根据评估结果，报告应酌情附有对本条例的修订建议。报告应予以公布。
3. 第2款提及的报告应特别关注以下方面：
(a) 各国主管机关为有效履行本条例赋予它们的任务而拥有的财力、技术和人力资源状况；
(b) 成员国对违反本条例规定的行为的处罚情况，特别是第71条第1款所指的行政罚款。
(ba) 为支持本条例而采用的统一标准和共同规格。
(bb) 条例生效后进入市场的公司数量，其中有多少是小微型企业。
(bb) 在第85条第2款提及的本条例生效之日起两年内，欧盟委员会应评估人工智能办公室的运作情况，该办公室是否已被赋予足够的权力和权限以完成其任务，以及是否有必要和有必要提升该办公室及其执行权限并增加其资源，以适当实施和执行本条例。欧盟委员会将向欧洲议会和欧盟理事会提交该评估报告。
3a. 在第85条第2款所述本条例实施之日起两年内，以及此后每四年，欧盟委员会应提交一份关于通用模型节能开发标准化交付成果进展情况的审查报告，并评估是否需要采取进一步措施或行动，包括具有约束力的措施或行动。该报告应提交给欧洲议会和理事会，并应公布于众。
4. 在第85条第2款所述本条例实施之日起两年内，以及此后每三年，委员会应评估自愿行为守则的影响和有效性，以促进第三编第2章对高风险人工智能系统以外的人工智能系统的要求以及可能对高风险人工智能系统以外的人工智能系统的其他额外要求的实施，包括在环境可持续性方面；
5. 为第1款至第4款之目的，欧洲人工智能委员会、成员国和国家主管机关应按

委员会的要求向其提供信息，不得无故拖延。
6. 在进行第1款至第4款所述的评估和审查时，委员会应考虑欧洲人工智能委员会、欧洲议会、欧盟理事会以及其他相关机构或来源的立场和结论。
7. 如有必要，委员会应提交适当的建议来修订本条例，特别是要考虑到技术的发展、人工智能系统对健康和安全的影响、基本权利以及信息社会的进步状况。
7a. 为指导本条第1款至第4款所述的评估和审查工作，人工智能办公室应承诺制定一种客观的、参与性的方法，用于根据相关条款所列的标准评估风险水平，并将新的系统列入：
附件三清单，包括扩展该附件中现有的领域或增加新的领域；
第5条规定的禁止实践清单；以及
根据第52条需要采取额外透明度措施的人工智能系统清单。
7b. 根据本条第7款对本条例的任何修正，或今后涉及附件二B节所列部门立法的相关授权法案或实施法案，均应考虑到各部门的监管特点，以及现有的管理、合格性评估和执行机制以及在这些部门建立的主管机构。
7c. 自本条例实施之日起五年内，欧盟委员会应对本条例的实施情况进行评估，并向欧洲议会、欧盟理事会和欧洲经济和社会委员会报告，同时考虑到本条例最初若干年的实施情况。在评估结果的基础上，该报告应酌情附有关于本条例执行结构的修订建议，以及是否需要设立一个联盟机构来解决任何已经查明的缺陷。

第85条
生效和适用

1. 本条例自其在《欧洲联盟公报》上公布后第20天起生效。
2. 本条例自生效后24个月起适用。关于第53条第1款提及的义务，该义务应涵盖每个成员国在适用当天至少有一个监管沙盒投入运行，或者该成员国参与了另一个成员国的沙盒。
3. 克减第2款：
(a) 第一编和第二编自本条例生效后六个月起适用；
(a) 第三编第4章、第6章、第8a章和第10章应在本条例生效后十二个月起适用；
(b) 第6条第1款和本条例中的相应义务自本条例生效后36个月起适用。
行为守则最迟应在本条例生效后九个月编制完成。人工智能办公室应采取必要的措施，包括根据第52e条第5款邀请提供者。
本条例以其整体具备约束力，并直接适用于所有成员国。

在布鲁塞尔定稿，

欧洲议会
主席

欧盟理事会
主席

附件二
联盟统一立法清单

A部分 - 基于新立法框架的联盟统一立法清单

1.欧洲议会和欧盟理事会2006年5月17日关于机械的2006/42/EC号指令，修订95/16/EC号指令（官方公报，L 157，2006年6月9日，第24页）[为机械条例所废除]；
2.欧洲议会和理事会2009年6月18日关于玩具安全的2009/48/EC号指令（官方公报，L 170，2009年6月30日，第1页）；
3.欧洲议会和欧盟理事会2013年11月20日关于休闲艇和个人水上摩托艇并废除94/25/EC号指令的2013/53/EU号指令（官方公报，L 354，2013年12月28日，第90页）；
4.欧洲议会和欧盟理事会2014年2月26日关于协调成员国电梯和电梯安全组件相关法律的2014/33/EU号指令（官方公报，L 96，2014年3月29日，第251页）；
5.欧洲议会和欧盟理事会2014年2月26日关于统一成员国有关在潜在爆炸性气体环境中使用的设备和保护系统的法律的2014/34/EU号指令（官方公报，L 96，2014年3月29日，第309页）；
6.欧洲议会和欧盟理事会2014年4月16日关于统一成员国有关无线电设备市场准入的法律并废除1999/5/EC号指令的2014/53/EU号指令（官方公报，L 153，2014年5月22日，第62页）；
7.欧洲议会和欧盟理事会2014年5月15日关于协调成员国有关压力设备市场销售的法律的2014/68/EU号指令（官方公报，L 189，2014年6月27日，第164页）；
8.欧洲议会和欧盟理事会2016年3月9日关于缆道装置并废除2000/9/EC号指令2016/424号条例（官方公报，L 81，2016年3月31日，第1页）；
9.欧洲议会和欧盟理事会2016年3月9日关于个人防护设备并废除理事会89/686/EEC号指令的2016/425号条例（官方公报，L 81，2016年3月31日，第51 页）；
10.欧洲议会和欧盟理事会2016年3月9日关于燃烧气体燃料的器具并废除2009/142/EC号指令的2016/426号条例（官方公报，L 81，2016年3月31日，第99页）；
11.欧洲议会和欧盟理事会2017年4月5日关于医疗器械的2017/745号条例，修订2001/83/EC号指令、178/2002号条例和1223/2009号条例，并废除了90/385/EEC号和93/42/EEC号理事会指令（官方公报，L 117，2017年5月5日，第1页）；
12.欧洲议会和欧盟理事会2017年4月5日关于体外诊断医疗器械的2017/746号条例，废除98/79/EC号指令和2010/227/EU号委员会决定（官方公报，L 117，2017年5月5日，第176页）。

B. 联盟其他统一立法清单

13.欧洲议会和欧盟理事会2008年3月11日关于民用航空安全领域共同规则的300/2008号条例，废除2320/2002号条例（官方公报，L 97，2008年4月9日，第72页）。
14.欧洲议会和欧盟理事会2013年1月15日关于两轮或三轮汽车和四轮车审批和市场监督的168/2013号条例（官方公报，L 60，2013年3月2日，第52页）；
15.欧洲议会和欧盟理事会2013年2月5日关于农林车辆审批和市场监管的

167/2013号条例（官方公报，L 60，2013年3月2日，第1页）；
16.欧洲议会和欧盟理事会2014年7月23日关于海洋设备的2014/90/EU号指令，废除理事会96/98/EC号指令（官方公报，L 257，2014年8月28日，第146页）；
17.欧洲议会和欧盟理事会2016年5月11日关于欧盟内部铁路系统互操作性的2016/797号指令（官方公报，L 138，2016年5月26日，第44页）。
18.欧洲议会和欧盟理事会2018年5月30日关于机动车辆及其挂车以及用于此类车辆的系统、组件和独立技术单元的审批和市场监督的2018/858号条例，修订715/2007号和595/2009号条例，并废止了2007/46/EC号指令（官方公报，L 151，2018年6月14日，第1页）；
18a.欧洲议会和欧盟理事会2019年11月27日2019/2144号条例，关于机动车辆及其挂车，以及用于此类车辆的系统、组件和独立技术单元在一般安全和保护车内人员及易受伤害的道路使用者方面的类型批准要求，修订欧洲议会和欧盟理事会2018/858号条例，并废除欧洲议会和欧盟理事会78/2009号条例、79/2009号条例和661/2009号条例，以及欧盟委员会631/2009号条例、406/2010号条例和661/2010号条例、欧洲议会和欧盟理事会78/2009号、79/2009号和(EC) 661/2009号条例，以及欧盟委员会631/2009号、406/2010号、672/2010号、1003/2010号、1005/2010号条例、1008/2010号、1009/2010号、19/2011号、109/2011号、458/2011号、65/2012号、130/2012号、347/2012号、351/2012号、1230/2012号和 2015/166号条例(官方公报，L 325，2019年12月16日，第1页)；
19.欧洲议会和理事会2018年7月4日关于民用航空领域共同规则和建立欧盟航空安全局的2018/1139号条例，修订2111/2005号、1008/2008号、996/2010号条例、376/2014号以及欧洲议会和理事会2014/30/EU和2014/53/EU号指令，并废除欧洲议会和理事会条例552/2004号和216/2008号以及理事会3922/91号条例（官方公报，L 212，2018年8月22日，第1页），就其第2条第1款第a和b点所述飞机的设计、生产和投放市场而言，涉及无人驾驶飞机及其发动机、螺旋桨、零组件和遥控设备。

附件二a
第5条第1款第3项所述的刑事犯罪清单——恐怖主义、

- 贩卖人口
- 对儿童的性剥削和儿童色情制品
- 非法贩运麻醉药品和精神药物
- 非法贩运武器、弹药和爆炸物
- 谋杀、严重人身伤害
- 人体器官和组织的非法贸易
- 非法贩运核材料或放射性材料
- 绑架、非法限制人身自由和劫持人质
- 国际刑事法院管辖范围内的罪行
- 非法扣押飞机/船只
- 强奸
- 环境犯罪
- 有组织或武装抢劫

- 破坏
- 参与涉及上述一种或多种罪行的犯罪组织

附件三
第6条第2款提及的高风险人工智能系统

第6条第2款所指的高风险人工智能系统是指下列任何一个领域所列的人工智能系统：
1. 生物识别技术，只要相关欧盟或国家法律允许使用：
(a) 远程生物识别系统。
这不包括用于生物验证的人工智能系统，其唯一目的是确认特定自然人就是他或她声称的那个人；
(aa) 根据敏感或受保护的属性或特征，基于对这些属性或特征的推断，意图用于生物鉴别分类的人工智能系统。
(ab) 拟用于情感识别的人工智能系统；
2. 关键基础设施：
(a) 拟用作重要数字基础设施、道路交通以及水、气、暖和电供应的管理和运行的安全组件的人工智能系统。
3. 教育和职业培训：
(a) 用于确定自然人进入各级教育和职业培训机构或课程的机会、录取或分配的人工智能系统；
(b) 拟用于评估学习成果的人工智能系统，包括当这些成果被用于指导各级教育和职业培训机构中自然人的学习过程时。
(ba) 在教育和职业培训机构内，用于评估个人将接受或能够接受的适当教育水平的人工智能系统；
(bb) 在教育和职业培训机构内，用于监控和检测学生考试违纪行为的人工智能系统；
4. 就业、工人管理和自营职业：
(a) 用于招聘或选拔自然人的人工智能系统，特别是用于发布有针对性的招聘广告、分析和过滤求职申请以及评估候选人；
(b) AI 旨在用于做出影响工作相关关系、晋升和终止工作相关合同关系条款的决定，根据个人行为或个人特质或特征分配任务，以及监督和评估此类关系中人员的绩效和行为；
5. 获得和享受基本私人服务以及基本公共服务和福利：
(a) 拟由公共机关或代表公共机关使用的人工智能系统，以评估自然人获得基本公共援助福利和服务，包括医疗保健服务，的资格，以及发放、减少、撤销或收回此类福利和服务；
(b) 拟用于评估自然人信用度或确定其信用评分的人工智能系统，但用于侦查金融欺诈的人工智能系统除外；
(c) 用于对自然人的紧急呼叫进行评估和分类的人工智能系统，或用于调度或确定调度紧急应急服务，包括警察、消防员和医疗救助，的优先次序的人工智能系统，以及紧急医疗保健病人的分流系统；
(ca) 在人寿保险和健康保险方面，拟用于自然人风险评估和定价的人工智能系统

6. 执法部门，只要相关欧盟或国家法律允许使用：
(a) 供执法机关或代表执法机关使用的人工智能系统，或供支持执法机关或代表执法机关的联盟机构、机关、办公室或团体使用的人工智能系统，以评估自然人成为刑事犯罪受害者的风险；
(b) 拟由执法机关或代表执法机关使用的人工智能系统，或拟由联盟机构、团体和机关支持执法机关使用的人工智能系统，如测谎仪和类似工具；
(d) 供执法机关或代表执法机关使用的人工智能系统，或供支持执法机关的联盟机构、机关、办公室或团体使用的人工智能系统，以便在调查或起诉刑事犯罪过程中评估证据的可靠性；
(e) 供执法机关或代表执法机关或欧盟机构、机关、办公室或支持执法机关的机构使用的人工智能系统，用于评估自然人的犯罪或再犯罪风险，而不仅仅是基于2016/680指令第3条第4点所述的自然人画像，或者用于评估自然人或群体的个性特征和特点或过去的犯罪行为；
(f) 在侦查、调查或起诉刑事犯罪的过程中，意图由执法机关或代表执法机关或由支持执法机关的联盟机构、机关、办公室或团体使用的人工智能系统，用于2016/680指令第3条第4点所述的自然人画像。
7. 移民、庇护和边境控制管理，只要相关联盟或国家法律允许使用：
(a) 供主管公共机关用作测谎和类似工具的人工智能系统；
(b) 供主管公共机关或联盟机构、办公室或机关或代表主管公共机关或联盟机构、办公室或机关使用的人工智能系统，以评估拟进入或已进入成员国领土的自然人带来的风险，包括安全风险、非正常移民风险或健康风险；
(d) 拟由主管公共机关或代表主管公共机关或由联盟机构、办公室或机关使用的人工智能系统，以协助主管公共机关审查庇护、签证和居留许可申请以及与申请身份的自然人的资格有关的相关投诉，包括对证据可靠性的相关评估；
(da) 在移民、庇护和边境管制管理方面，意图由主管公共机关，包括欧盟机构、办公室或团体，或代表其使用的人工智能系统，目的是检测、识别 或辨认自然人，但旅行证件核查除外；
8. 司法和民主进程：
(a) 拟由司法机关或代表司法机关使用的人工智能系统，以协助司法机关研究和解释事实和法律，并将法律适用于一组具体事实；
(aa) 拟用于影响选举或全民投票结果或自然人在选举或全民投票中行使投票权的投票行为的人工智能系统。这不包括自然人不直接接触其输出结果的人工智能系统，例如从行政和后勤角度用于组织、优化和结构化政治运动的工具。

附件四
第11条第1款提及的技术文件

第11条第1款所指的技术文件应至少包含适用于相关人工智能系统的以下信息：
1. 人工智能系统的总体描述，包括
(a) 系统的预期目的、提供者的名称以及系统的版本（反映其与以前版本的关系）；
(b) 在适用情况下，人工智能系统如何与不属于人工智能系统本身的硬件或软件（包括其他人工智能系统）进行交互或可用于与之进行交互；
(c) 相关软件或固件的版本以及与版本更新有关的任何要求；

(d) 说明人工智能系统投放市场或投入使用的所有形式（如嵌入硬件的软件包、可下载的软件包、API等）；
(e) 说明人工智能系统意图在哪些硬件上运行；
(f) 如果人工智能系统是产品的一个组成部分，展示这些产品的外部特征、标记和内部布局的照片或插图；
(fa) 向部署者提供的用户界面的基本描述；
(g) 部署者的使用说明和向部署者提供的用户界面的基本说明（如适用）；
2.详细描述人工智能系统的要素及其开发过程，包括
(a) 开发人工智能系统所采用的方法和步骤，包括在相关情况下使用第三方提供的预训练系统或工具，以及提供者如何使用、整合或修改这些系统或工具；
(b) 系统的设计规格，即人工智能系统和算法的一般逻辑；关键的设计选择，包括所依据的理由和所作的假设，也包括系统意图用于哪些人或哪些群体；主要的分类选择；系统旨在优化的目标，以及不同参数的相关性；系统预期输出的说明；为遵守第三编第2章的要求而采用的技术解决方案的任何可能的权衡取舍决定；
(c) 系统结构说明，解释软件组件如何相互依存或相互促进，以及如何集成到整个处理过程中；用于开发、训练、测试和验证人工智能系统的计算资源；
(d) 在相关情况下，以数据表的形式提供数据要求，说明培训方法和技术以及所使用的培训数据集，包括这些数据集的一般说明，有关其来源、范围和主要特征的信息；数据是如何获得和选择；标注程序（例如监督学习）、数据清理方法（例如异常值检测）；
(e) 根据第14条评估所需的人工监督措施，包括根据第13条第3款第d项评估所需的技术措施，以便于部署者解释人工智能系统的输出结果；
(f) 在适用的情况下，详细描述对人工智能系统及其性能预先确定的更改，以及与为确保人工智能系统持续符合第三编第2章规定的相关要求而采取的技术解决方案有关的所有信息；
(g) 所使用的验证和测试程序，包括关于所使用的验证和测试数据及其主要特征的信息；用于衡量准确性、稳健性和是否符合第三编第2章规定的其他相 关要求以及潜在歧视性影响的指标；测试日志和所有测试报告，包括第f点所述的预先确定的更改，须注明日期并由负责人签字。
(ga) 网络安全措施的到位。
3.关于人工智能系统的监测、运作和控制的详细资料，特别是以下方面的资料其性能方面的能力和局限性，包括该系统意图对之使用的特定个人或群体的准确度，以及与其预期目的相关的总体预期准确度；鉴于人工智能系统的预期目的，可预见的意外结果以及对健康和安全、基本权利和歧视的风险来源；根据第14条所需的人为监督措施，包括为便于部署者解释人工智能系统的输出结果而采取的技术措施；输入数据的规格（视情况而定）；
3.说明性能指标是否适合特定的人工智能系统；
4.根据第9条对风险管理系统的详细说明；
5.描述提供者在系统生命周期内对系统所做的相关更改；
6.全部或部分采用的统一标准清单，其参考文件已在《欧盟官方公报》上公布；如未采用此类统一标准，应详细说明为满足第三编第2章规定的要求而采用的解决方案，包括所采用的其他相关标准和技术规范的清单；
7.欧盟合格性声明副本；

8.详细说明根据第61条为评估人工智能系统在后市场阶段的性能而建立的系统，包括第61条第3款所述的后市场监测计划。

附件五
欧盟合格性声明

第48条提及的欧盟合格性声明应包含以下所有信息：
1.人工智能系统的名称和类型，以及可识别和追溯人工智能系统的任何其他明确参考信息；
2.提供者或其授权代表（如适用）的姓名和地址；
3.欧盟合格性声明由提供者全权负责签发的声明；
4.一份声明，说明有关人工智能系统符合本条例，并在适用的情况下，符合任何其他规定签发欧盟合格性声明的相关欧盟立法；
4a.如果人工智能系统涉及个人数据处理，则应声明该人工智能系统符合2016/679和2018/1725号条例以及2016/680号指令。
5.所使用的任何相关统一标准或任何其他通用规范的参考文件，声明与之相符；
6.在适用的情况下，提供通知机关的名称和标识号、所执行的合格性评估程序的说明以及所颁发认证的标识；
7.声明的签发地点和日期、签署人的姓名和职务，并注明其代表和被代表人。

附件六
基于内部控制的合格性评估程序

1.基于内部控制的合格性评估程序是基于第2至4点的合格性评估程序。
2.提供者核实已建立的质量管理体系符合第17条的要求。
3.提供者审查技术文件中的信息，以评估人工智能系统是否符合第三编第2章规定的相关基本要求。
4.提供者还要核实人工智能系统的设计和开发过程以及第61条所述的后市场监测与技术文件相一致。

附件七
基于质量管理体系评估和技术文件评估的合格性

1.引言 基于质量管理体系评估和技术文件评估的合格性评估是基于第2至5点的合格性评估程序。
2.概述 第17条规定的经批准的设计、开发和测试人工智能系统的质量管理体系应根据第3点进行审查，并应接受第5点规定的监督。应根据第4点审查人工智能系统的技术文件。
3.质量管理系统
3.1.提供者的申请应包括：
(a) 提供者的姓名和地址，如果申请由授权代表提交，还需提供其姓名和地址；
(b) 同一质量管理体系所涵盖的人工智能系统清单；

(c) 同一质量管理体系所涵盖的每个人工智能系统的技术文件；
(d) 有关质量管理体系的文件，应涵盖第17条所列的所有方面；
(e) 为确保质量管理体系的充分性和有效性而制定的程序说明；
(f) 书面声明未向任何其他通知机构提交过同一申请。
3.2.通知机构应对质量管理体系进行评估，确定其是否满足第17条所述要求。该决定应通知提供者或其授权代表。通知应包含对质量管理体系的评估结论和合理的评估决定。
3.3.提供者应继续实施和维护经批准的质量管理体系，使其保持适当和有效。
3.4.对已获批准的质量管理体系或其所涵盖的人工智能系统清单的任何预期更改，应由提供者提请通知机构注意。通知机构应对拟议的更改进行审查，并决定修改后的质量管理体系是继续满足第3.2点所述要求，还是有必要进行重新评估。通知机构应将其决定通知提供者。通知应包含对修改的审查结论和合理的评估决定。
4.控制技术文件。
4.1.除第3点所述的申请外，提供者还应向其选择的通知机构提出申请，要求对与提供者意图投放市场或投入使用的人工智能系统有关的技术文件进行评估，该人工智能系统属于第3点所述质量管理系统的范围。
4.2.申请应包括
(a) 提供者的名称和地址；
(b) 一份书面声明，表明未向任何其他通知机构提交过同一申请；
(c) 附件四提及的技术文件。
4.3.技术文件应由通知机构审查。在相关和仅限于完成任务所必需的情况下，应允许通知机构完全访问所使用的培训、审定和测试数据集，包括在适当和有安全保障的情况下，通过应用编程接口（API）或其他相关技术手段和工具进行远程访问。
4.4.在审查技术文件时，通知机构可要求提供者提供进一步的证据或进行进一步的测试，以便适当评估人工智能系统是否符合第三编第2章的要求。如果通知机构对提供者进行的测试不满意，通知机构应酌情直接进行适当的测试。
4.5.为评估高风险人工智能系统是否符合第三编第2章规定的要求，在已用尽所有其他合理的核查合格性的方法并证明不充分之后，如有必要，经合理请求，还应允许通知机构查阅人工智能系统的训练和训练模型，包括其相关参数。这种查阅应遵守欧盟关于知识产权和商业秘密保护的现行法律。
4.6.该决定应通知提供者或其授权代表。通知应包含技术文件的评估结论和合理的评估决定。
如果人工智能系统符合第三篇第二章规定的要求，通知机构应颁发欧盟技术文件评估认证。认证应注明提供者的名称和地址、检查结论、有效条件（如有）以及识别人工智能系统的必要数据。
认证及其附件应包含所有相关信息，以便对人工智能系统的合格性进行评估，并在适用情况下对使用中的人工智能系统进行控制。
如果人工智能系统不符合第三编第2章规定的要求，通知机构应拒绝签发欧盟技术文 件评估认证，并应相应地通知申请人，详细说明拒绝的理由。
如果人工智能系统不符合与用于训练该系统的数据有关的要求，则需要在申请新的合格性评估之前重新训练人工智能系统。在这种情况下，通知机构拒绝签发欧盟技术文件评估认证的合理评估决定应包含对用于训练人工智能系统的质

量数据的具体考虑，特别是不符合要求的原因。
4.7.对人工智能系统的任何修改，如可能影响人工智能系统符合要求或其预期目的，应得到颁发欧盟技术文件评估认证的通知机构的批准。提供者应将其引入任何上述变更的意向，或以其它方式了解到发生此类变更的情况，通知上述通知机构。通知机构应评估意图进行的更改，并决定这些更改是否需要根据第43条第4款进行新的合格性评估，或是否可以通过对欧盟技术文件评估认证进行补充来解决。在后一种情况下，通知机构应评估变更，将其决定通知提供者，如果变更获得批准，则向提供者签发欧盟技术文件评估认证的补充文件。
5.对批准的质量管理体系进行监督。
5.1.第3点中提及的通知机构进行监督的目的是确保提供者充分履行经批准的质量管理体系的条款和条件。
5.2.为评估目的，提供者应允许通知机构进入设计、开发和测试人工智能系统的场所。提供者还应与通知机构共享所有必要信息。
5.3.通知机构应进行定期审核，以确保提供者维护和应用质量管理体系，并应向提供者提供审核报告。在审计过程中，通知机构可对已获得欧盟技术文件评估认证的人工智能系统进行额外测试。

附件八
根据第51条登记高风险人工智能系统时应提交的信息

A部分——对于根据第51条第1款登记的高风险人工智能系统，应提供以下信息并不断更新。
1.提供者的名称、地址和联系方式；
2.由他人代表提供者提交信息时，应提供该人的姓名、地址和联系方式；
3.授权代表的姓名、地址和联系方式（如适用）；
4.人工智能系统的商品名称和任何其他可识别和追溯人工智能系统的明确参考文件；
5.说明人工智能系统的预期目的以及通过该人工智能系统支持的组件和功能；
5a 系统使用的信息（数据、输入）及其运行逻辑的基本简明描述。
6.人工智能系统的状态（投放市场或投入使用；不再投放市场/投入使用；召回）；
7.通知机关颁发的认证的类型、编号和有效期，以及该通知机关的名称或识别号（如适用）；
8.第6点所述认证的扫描件（如适用）；
9.人工智能系统正在或已经投放市场、投入使用或在欧盟提供的成员国；
10.第48条提及的欧盟合格性声明副本；
11.电子使用说明；附件三第1、6和7点所述执法和移民、庇护和边境管制管理领域的高风险人工智能系统不得提供此类信息。
12.其他信息的 URL（可选）。

B部分——对于根据第51条登记的高风险人工智能系统，应提供并不断更新以下信息。
1. 部署者的姓名、地址和联系方式；
2. 代表部署者提交信息者的姓名、地址和联系方式；

5. 根据第29a条进行的基本权利影响评估的结论摘要
6.人工智能系统提供者在欧盟数据库中输入的 URL。
7.根据2016/679 号条例第35条或本条例第29条第6款规定的2016/680号指令第27条进行的数据保护影响评估（如适用）的摘要。

C部分——对于根据第51条第1a款登记的人工智能系统，应提供并不断更新以下信息。
1.提供者的名称、地址和联系方式；
1.由他人代表提供者提交信息时，应提供该人的姓名、地址和联系方式；
2.授权代表的姓名、地址和联系方式（如适用）；
3.人工智能系统的商品名称和任何其他可识别和追溯人工智能系统的明确参考文件；
4.说明人工智能系统的预期用途；
5.根据第6条第2a款规定的哪一条或哪一些标准，认为人工智能系统不是高风险系统；
6.根据第6条第2a款规定的程序将人工智能系统视为非高风险系统的理由简述；
7.人工智能系统的状态（投放市场或投入使用；不再投放市场/投入使用；召回）；人工智能系统正在或已经投放市场、投入使用或在欧盟提供的成员国。

附件八a
附件三所列高风险人工智能系统登记时应提交的关于按照第54条a款在真实世界进行测试的信息

根据第54a条的规定，应提供并不断更新在实际条件下进行测试的信息：
1.全联盟唯一的单一识别码，用于在实际条件下进行测试；
2.在真实条件下参与测试的提供者或潜在提供者及用户的名称和详细联系信息；
3.人工智能系统的简要说明、预期用途以及识别该系统所需的其他信息；
4.总结在实际条件下进行测试的计划的主要特点；
5.在实际条件下中止或终止测试的信息。

附件九
联盟关于自由、安全和司法领域大型信息系统的立法

1.申根信息系统
(a)欧洲议会和理事会2018年11月28日关于使用申根信息系统遣返非法居留的第三国国民的2018/1860条例（官方公报，L 312，2018年12月7日，第1页）。
(b)欧洲议会和欧盟理事会2018年11月28日关于在边境检查领域建立、运行和使用申根信息系统（SIS）的2018/1861号条例，修订《申根协定实施公约》，并修订和废止1987/2006 号条例（官方公报，L 312，2018年12月7日，第14页）
(c)欧洲议会和欧盟理事会2018年11月28日关于在警务合作和刑事司法合作领域建立、运行和使用申根信息系统（SIS）的2018/1862号条例，修订并废止理事会2007/533/JHA号决定，并废止欧洲议会和欧盟理事会1986/2006号条例和欧盟委员会2010/261/EU号决定（官方公报，L 312，2018年12月7日，第56页）。

2.签证信息系统
(a) 关于欧洲议会和欧盟理事会条例的建议，修订767/2008号条例、810/2009号条例、2017/2226号条例、2016/399号条例、XX/2018号条例[互操作性条例]和2004/512/EC号决定，并废除理事会2008/633/JHA号决定 - COM(2018) 302终稿。将在共同立法者通过条例（2021年4月/5月）后更新。
3.Eurodac
(a) 关于建立“Eurodac”的欧洲议会和欧盟理事会条例的修正提案，该“Eurodac”用于比对生物识别数据，以有效适用XXX/XXX号条例[庇护和移民管理条例]和XXX/XXX号条例[重新安置条例]、用于识别非法居留的第三国国民或无国籍人士，以及成员国执法机关和欧洲刑警组织为执法目的提出的与Eurodac数据进行比对的请求，并修订2018/1240号和2019/818号条例 - COM(2020) 614终稿。
4.出入口系统
(a) 欧洲议会和欧盟理事会2017年10月30日2017/2226号条例建立了出入境系统（EES），用于登记跨越成员国外部边界的第三国国民的出入境数据和拒绝入境数据，并确定了为执法目的访问出入境系统的条件，同时修订《申根协定实施公约》以及767/2008 号条例和1077/2011 号条例（官方公报，L 327，2017年12月9日，第20页）。
5.欧洲旅行信息和授权系统
(a)欧洲议会和欧盟理事会2018年9月12日关于建立欧洲旅行信息和授权系统（ETIAS）的2018/1240号条例，并修订1077/2011号、515/2014号、2016/399号、2016/1624号和2017/2226号条例（官方公报，L 236，19.9.2018，第1页）。
(b) 欧洲议会和欧盟理事会2018年9月12日2018/1241 号条例修订了2016/794号条例，旨在建立欧洲旅行信息和授权系统（ETIAS）（官方公报，L 236，2018年9月19日，第72页）。
6.关于第三国国民和无国籍人士的欧洲犯罪记录信息系统
(a) 欧洲议会和欧盟理事会2019年4月17日2019/816 号条例建立了一个中央系统，用于识别持有第三国国民和无国籍人士定罪信息的成员国（ECRIS-TCN），以补充欧洲犯罪记录信息系统，并修订2018/1726 号条例（官方公报，L 135，2019年5月22日，第1页）。
7.互操作性
(a) 欧洲议会和欧盟理事会2019年5月20日关于在边境和签证领域建立欧盟信息系统互操作性框架的2019/817号条例（官方公报L 135，2019年5月22日，第27页）。
(b)欧洲议会和欧盟理事会2019年5月20日关于在警察和司法合作、庇护和移民领域建立欧盟信息系统互操作性框架的第 2019/818 号条例（官方公报L 135，2019年5月22日，第85页）。

附件九a
第C条第1a款提及的技术文件

为通用人工智能模型提供者提供技术文档：

第1部分：所有通用人工智能模型提供者应提供的信息
第X条第b款所指的技术文件应至少包括与模型的规模和风险状况相适应的以下信息：
1.通用人工智能模型的一般描述，包括
a）模型将要执行的任务，以及可将其集成到其中的人工智能系统的类型和性质；
b）适用的可接受使用政策；
c）发布日期和分发方法；
d）结构和参数数量；
e）输入和输出的模式（如文本、图像）和格式；
f）许可；
2.详细描述第1款所述模型的要素，以及开发过程的相关信息，包括以下要素：
a）将通用人工智能模型纳入人工智能系统所需的技术手段（如使用说明、基础设施、工具）；
b）模型和训练过程的设计规范，包括训练方法和技术、关键设计选择（包括理由和假设）；模型设计的优化目标以及不同参数的相关性（如适用）；
c）用于培训、测试和验证的数据信息（如适用），包括数据类型和来源、整理方法（如清理、过滤等）、数据点的数量、范围和主要特征；数据的获取和选择方式，以及检测数据源不适合性的所有其他措施和检测可识别偏差的方法（如适用）；
d）训练模型所用的计算资源（如浮点运算次数FLOPs）、训练时间以及与训练有关的其他相关细节；
e）已知或估计的模型能耗；如果不知道，可根据所用计算资源的信息来确定；

第2部分：具有系统风险的通用人工智能模型提供者应提供的补充信息
3.根据现有的公共评价规程和工具或其他评价方法，详细描述评价策略，包括评价结果。评估策略应包括评估标准、衡量标准和确定局限性的方法。
4.在适用情况下，详细说明为进行内部和/或外部对抗测试（如蓝军）、模型调整（包括对齐和微调）而采取的措施。
在适用的情况下，详细描述系统结构，解释软件组件如何相互构建或反馈，以及如何集成到整体处理过程中。

附件九b
第C条第1b款提及的透明度信息

第X条第c款所述信息应至少包含以下内容：
1.通用人工智能模型的一般描述，包括
a）模型要执行的任务，以及可将其集成到其中的人工智能系统的类型和性质；
b）适用的可接受使用政策；
c）发布日期和分发方法；
d）模型如何与不属于模型本身的硬件或软件（如适用）进行交互或可用于与之进行交互；
e）与使用通用人工智能模型有关的相关软件版本（如适用）；
f）结构和参数数量、

g) 输入和输出的模式（如文本、图像）和格式；
h) 模型的许可；
2.模型要件及其开发过程的说明，包括
a) 将通用人工智能模型纳入人工智能系统所需的技术手段（如使用说明、基础设施、工具）。
b) 输入和输出的模式（如文本、图像等）和格式及其最大尺寸（如上下文窗口长度等）；
c) 用于培训、测试和验证的数据信息（如适用），包括数据类型和来源以及保存方法。

附件九c

为确定通用人工智能模型是否具有与第A条第a和b点相同的能力或影响，委员会应考虑以下标准：
a. 模型参数的数量；
b. 数据集的质量或大小，例如通过词元来衡量；
c. 训练模型所用的计算量，以FLOPs衡量，或由其他变量组合表示，如估计的训练成本、估计的训练所需时间或估计的训练能耗；
d. 模型的输入和输出模式，如文本到文本（大型语言模型）、文本到图像、多模态，以及确定每种模式的高影响能力的最新阈值，以及输入和输出的具体类型（如生物序列）；
e. 模型能力的基准和评估，包括考虑无需额外培训的任务数量、学习新的独特任务的适应性、其自主程度和可扩展性、可使用的工具；
f. 由于其覆盖范围，对内部市场的影响很大，如已提供给至少10000个设立在联盟之内的注册企业用户，则应加以推定；
g. 注册的终端用户数量。