欧盟《人工智能法》译文全文

欧洲议会和欧盟理事会 (EU) 2024/1689 条例

2024 年 6 月 13 日

制定人工智能统一规则和修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139 和(EU) 2019/2144 以及指令 2014/90/EU、(EU) 2016/797 和(EU) 2020/1828(人工智能法案)

译者简介：丁晓东，中国人民大学法学院教授、未来法治研究院副院长。中山大学电子与通信工程专业学士，北京大学、耶鲁大学法学博士。转载请注明译者和出处。由于译者精力、时间和水平所限，本译稿的疏漏之处在所难免，欢迎对本译稿提出批评和意见，联系邮箱：dingruc@163.com . 感谢何泽昊、刘洁晨、杨浩然等同学承担的部分文字的校对和格式调整工作。

第一章

总则

第 1 条
主题

1.本条例旨在改善欧盟内部市场的运作，促进以人为中心、值得信赖的人工智能的应用，同时确保对《欧盟基本权利宪章》规定的包括民主、法治和环境保护在内的健康、安全、基本权利的高水平保护，使其免受欧盟内的人工智能系统的有害影响，并支持创新。

2.本条例规定了：
(a) 在欧盟市场上投放、投入服务和使用人工智能系统的统一规则；
(b) 对特定人工智能实践的禁止；
(c) 对高风险人工智能系统的具体要求以及此类系统运营者的义务；
(d) 特定人工智能系统的统一透明度规则；
(e) 通用人工智能模型投放市场的统一规则；
(f) 市场监测、市场监督、治理和执法的规则；
(g) 支持创新的措施，特别是中小型企业（包括初创企业）。

第 2 条
范围

1.本条例适用于：
(a) 在欧盟境内将投人工智能系统投放市场或投入服务，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) 在欧盟境内设立经营场所或位于欧盟境内的人工智能系统部署者；
(c) 在第三国设立经营场所或位于第三国的人工智能系统提供者和部署者，但其人工智能系统产生的输出在欧盟使用；
(d) 人工智能系统的进口商和分销商；
(e) 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服务的产品制造商；
(f) 在欧盟境外设立的提供者的授权代表；
(g) 位于欧盟境内的受影响者。

2.对于根据第 6 条第 1 段被列为高风险人工智能系统且涉及附录一中 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 6 条第 1 段、第 102 至 109 条和第 112 条。第 57 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，并且在任何情况下均不得影响成员国在国家安全方面的权限，无论成员国委托何种实体执行与这些权限相关的任务。
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、投入服务或使用的人工智能系统，无论是否经过修改，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市场上投放或投入服务的人工智能系统，如果其输出在欧盟内仅用于军事、防御或国家安全目的，无论从事这些活动的实体属于何种类型。

4.本条例不适用于第三国公共机构，也不适用于根据第 1 段属于本条例范围内的国际组织，如果这些机构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，但前提是该第三国或国际组织在保护基本权利和个人自由方面提供了充分的保障。

5.本条例不影响(EU)2022/2065 条例（《数字服务法》）第二章中关于中介服务提供者责任的条款的适用。

6.本条例不适用于专为科学研究和发展目的而开发和投入服务的人工智能系统或人工智能模型，包括其输出。
7.关于个人数据保护、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相关的被处理的个人数据。在不影响本条例第 10 条第 5 段和第 59 条适用的前提下，本条例不得影响 2016/679 条例 (GDPR) 或 2018/1725 条例或 2002/58/EC 指令或 2016/680/EU 指令的适用。

8.本条例不适用于在市场上投放或投用之前对人工智能系统或人工智能模型进行的任何研究、测试或开发活动。这类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。

9.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的规定。

10.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。

11.本条例不妨碍欧盟或成员国保留或引入在涉及到雇主使用人工智能系统的保护工人权利方面对工人更有利的法律、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。

12.本条例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 5 条或第 50 条的人工智能系统投放市场或投入服务。

第 3 条
定义

从本条例目的出发，适用以下定义：

(1) “人工智能系统”是指设计用于以不同程度的自主性运行，并可能在部署后表现出适应性的机器系统，且为了明确或隐含的目标，根据其接收的输入中推断如何生成可以影响物理或虚拟环境的输出，如预测、内容、建议或决策；

(2) “风险”是指损害发生的可能性和损害的严重程度的结合；

(3) “提供者”是指开发人工智能系统或通用人工智能模型，或拥有已开发人工智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服务的自然人或法人、公共机关、机构或其他组织，无论是收费还是免费；

(4) “部署者”是指在其权限下使用人工智能系统的自然人或法人、公共机关、机构或其他组织，但将人工智能系统用于个人非职业活动的除外；

(5) “授权代表”是指位于或设立在欧盟的自然人或法人，已接收并接受来自人工智能系统或通用人工智能模型提供者的书面授权书，分别代表其履行和执行本条例规定的义务和程序；

(6) “进口商”是指位于欧盟或在欧盟境内设立或位于欧盟的自然人或法人，在市场上投放带有第三国自然人或法人的名称或商标的人工智能系统；

(7) “分销商”是指供应链中除提供者或进口商外，在欧盟市场中提供人工智能系统的自然人或法人；

(8) “运营者”是指提供者、产品制造商、部署者、授权代表、进口商或分销商；

(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，供在欧盟市场上销售或使用，无论是付费的还是收费的；

(11) “投入服务”是指将人工智能系统直接提供给部署者首次使用，或供其在欧盟内按照预期目的自用；

(12) “预期目的”是指提供者拟用于人工智能系统的用途，包括提供者在使用说明、宣传或销售材料和声明以及技术文档中提供的信息中规定的特定场景和使用条件；

(13) “合理可预见的误用”是指不符合其预期用途的人工智能系统的使用，但可能由合理可预见的人类行为或与其他系统（包括其他人工智能系统）的互动引起；

(14) “安全组件”是指产品或人工智能系统的组成部分，履行产品或人工智能系统的安全功能，或其故障或失灵会危及健康和人身或财产安全；

(15) “使用说明”是指提供者特别为告知部署者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”是指任何旨在把提供给部署者的人工智能系统返还给提供者，或使其停止服务，或禁止其使用的措施。

（17）“人工智能系统的撤回”是指任何旨在防止在供应链系统中在市场上提供人工智能系统的措施；

（18）“人工智能系统的性能”是指人工智能系统实现其预期用途的能力；

（19）“通知机关”是指负责设立和执行必要程序以评估、指定和通知合格评估机构并进行监督的各成员国的国家机关；

（20）“合格性评估”是指证明高风险人工智能系统符合本条例第三章第二节规定的要求的过程；

（21）“合格性评估机构”是指执行第三方合格评估活动的机构，包括测试、认证和检验；

（22）“被通知机构”是指根据本条例和其他相关欧盟统一立法被通知的合格性评估机构；

（23）“实质性修改”是指人工智能系统在投放市场或投入服务后发生的修改，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对本条例第三章第二节规定要求的合规性，或导致人工智能系统被评估的预期目的发生修改；

（24）“CE 合格性标志”是指提供者表明人工智能系统符合第三章第二节中规定的要求以及其他适用的欧盟统一立法规定的要求的标志；

（25）“后市场监测系统”是指提供者为收集和审查其投放市场或投入服务的人工智能系统使用经验以确定是否需要立即采取必要的纠正或预防措施而进行的所有活动；

（26）“市场监督管理机关”是指根据(EU)2019/1020 条例开展活动和采取措施的国家机关；

（27）“统一标准”是指根据欧盟 1025/2012 号条例第 2 条第 1 段(c)项定义的统一标准；

（28）“共同规格”是指 1025/2012 号条例第 2 条第 4 段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” 指的是用于通过拟合可学习参数来训练人工智能系统的数据。；

（30）“验证数据”是指用于评估训练后的人工智能系统,并调整其不可学习参数和学习过程,以防止欠拟合或过拟合的数据；

（31）“验证数据集”是指单独的数据集或训练数据集的一部分，无论是以固定还是可变方式划分；

（32）“测试数据”是指用于在人工智能系统投放市场或投入服务前进行独立评估以确认其预期性能的数据；

（33）“输入数据”是指提供给人工智能系统或由其直接获取的、基于这些数据系统产生输出的数据；

（34）“生物识别数据”是指经过特定技术处理的个人数据，涉及自然人的物理、生理或行为特征，例如面部图像或指纹数据；

（35）“生物识别”是指为了确定自然人身份，将个人的生物识别数据与存储在数据库中的个人的生物识别数据进行比较，而自动识别人类的生理、生理、行为或心理特征；

（36）“生物识别验证”是指通过将自然人提供的生物识别数据与之前提供的生物识别数据进行对比的自动化一对一验证过程,包括身份验证；

（37）“特殊类别的个人数据”是指(EU)2016/679 条例第 9 条第 1 段、(EU)2016/680 指令第 10 条和(EU)2018/1725 号条例第 10 条第 1 段中提到的个人数据类别；

（38）“敏感业务数据”是指涉及预防、侦查、调查或起诉刑事犯罪活动有关的业务数据，其披露可能危及刑事诉讼程序的完整性；

（39）“情感识别系统”是指旨在基于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；

(40) “生物识别分类系统”是指为了基于自然人的生物识别数据将其分配到特定类别的人工智能系统，除非其作为其他商业服务的辅助，而且完全出于客观技术原因具有必要性；

(41) “远程生物识别系统”是指通过将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对，通常在远距离自动识别自然人、且不需要其主动参与的人工智能系统；

(42) “实时远程生物识别系统”是指生物识别数据的采集、比较和识别均没有明显延迟的远程生物识别系统，不仅包括即时识别，还包括为了规避的有限短暂延迟；

(43) “后远程生物识别系统”是指非实时远程生物识别系统的远程生物识别系统；

(44) “公众可进入的场所”是指无论是否附加某些访问条件，无论潜在容量限制，均可供不特定人数的自然人访问的任何公开或私人拥有的物理场所；

(45) “执法机关”是指：

(a) 有权预防、调查、侦查或起诉刑事犯罪或执行刑罚的任何公共机关，包括防范和预防对公共安全的威胁；或

(b) 根据成员国法律赋予公共权威和公共权力的任何其他机构或实体，旨在预防、调查、侦查或起诉刑事犯罪或执行刑罚，包括防范和预防对公共安全的威胁；

(46) “执法”是指由执法机关或代表其进行的预防、调查、侦查或起诉刑事犯罪或执行刑罚的活动，包括防范和预防对公共安全的威胁；

(47) “人工智能办公室”是指欧盟委员会负责实施、监测和监督人工智能系统和通用人工智能模型及人工智能治理的职能，依据 2024 年 1 月 24 日的欧盟委员会决定建立的职能；本条例中提到的人工智能办公室应解释为指欧盟委员会；

(48) “成员国主管机关”是指通知机关或市场监督管理机关；对于欧盟机关、机构、办事处和其他实体投入服务或使用的人工智能系统，本条例所指的成员国主管机关或市场监督管理机关应解释为指欧洲数据保护监管机构；

(49) “严重事故”是指人工智能系统的事故或故障，直接或间接导致以下任何后果：

(a) 致人死亡或对个人健康的严重伤害；

(b) 对关键基础设施管理或操作造成的严重和不可逆转的破坏；

(c) 违反旨在保护基本权利的欧盟法律规定的义务；

(d) 对财产或环境的严重损害；

(50) “个人数据”是指 2016/679 条例第 4 条第 1 段定义的个人数据；

(51) “非个人数据”是指 2016/679 条例第 4 条第 1 段定义的个人数据以外的数据；

(52) “用户画像”是指(EU)2016/679 条例第 4 条第 4 段定义的用户画像；

(53) “真实世界测试计划”是指描述在真实世界条件下进行测试的目标、方法、地理范围、人口和时间范围、监测、组织和实施的文件；

(54) “沙盒计划”是指参与提供者与主管机关之间达成的协议，描述在沙盒内进行活动的目标、条件、时间框架、方法和要求；

(55) “人工智能监管沙盒”是指由主管机关设立的受控框架，该框架为人工智能系统的提供者或潜在提供者提供了合适现实条件下根据沙盒计划的规定，在有限时间内在监管监督下，开发、训练、验证和测试创新人工智能系统的可能性；

(56) “人工智能素养”是指提供者、部署者和受影响人员具备的技能、知识和理解，使他们能够在本条例的背景下根据其各自的权利和义务，做出知情的人工智能系统部署决策，并了解人工智能的机会、风险以及可能造成的危害；

(57) “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，临时测试人工智能系统在真实世界条件下的预期用途，以收集可靠和稳健的数据，并评估和验证人工智能系统是否符合本条例的要求，并且在满足本条例第 57 条或第 60 条规定的所有条件的前提下，不视为在市场上投放或投入使用人工智能系统；

(58) “测试主体”在真实世界测试中是指参与真实世界条件下测试的自然人；

(59) “知情同意”是指受试者在了解所有与其参与决策相关的测试方面信息后，自由作出地、特地、清晰和自愿地表示愿意参与特定真实世界条件下测试的表达；

(60) “深度伪造”是指人工智能生成或操纵的图像、音频或视频内容，类似于现有的人物、物体、地点、实体或事件，并且会使人错误地认为其是真的或真实的；

(61) “广泛侵权”是指违反保护个人利益的欧盟法律的任何行为或不作为，包括：

(a) 造成或可能造成至少两个成员国居民的集体利益受损，除了以下情况：

(i) 该行为或不作为源自成员国或发生在成员国；

(ii) 涉及的提供者或其授权代表处于或设立于成员国；或

(iii) 当侵权行为由部署者实施时，部署者是在成员国设立；

(b) 已经造成、正在造成或可能造成个人集体利益受损，并且具有共同特征，包括相同的违法行为或相同的受侵害利益，并且由同一运营者实施，至少在三个成员国同时发生；

(62) “关键基础设施”是指(EU)2022/2557 指令第 2 条第 4 段定义的关键基础设施；

(63) “通用人工智能模型”是指包括使用大量数据进行大规模自我监督训练的人工智能模型，无论该模型如何投放市场，都具有显著的普遍性和能够胜任各种不同的任务，并且可以集成到各种下游系统或应用中；除了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;

(64) “高影响能力”是指匹配或超过最先进的通用人工智能模型中所记录能力的能力；

(65) “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，这类风险由于其覆盖范围对欧盟市场产生重大影响，或者由于对公共健康、安全、公共安全、基本权利或整个社会产生实际或合理可预见的负面影响，可以在整个价值链中大规模传播;

(66) “通用人工智能系统”是指基于通用人工智能模型的人工智能系统，该系统可以服务于多种目的，即可以直接使用，也可以集成到其他人工智能系统中；

(67) “浮点运算”是指涉及浮点数的任何数学运算或赋值，浮点数是计算机上表示的实数子集，通常由固定精度的整数与固定基数的整数指数表示；

(68) “下游提供者”是指人工智能系统的提供者，包括集成人工智能模型的通用人工智能系统，无论该人工智能模型是由自身提供并进行垂直整合，还是基于合同关系由其他实体提供。

第 4 条
人工智能素养

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，尽其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素养。

第二章

禁止的人工智能实践

第 5 条
禁止的人工智能实践

1.下列人工智能实践应被禁止：

(a) 投放市场、投入服务或加以使用此类人工智能系统，即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) 投放市场、投入服务或加以使用此类人工智能系统，即利用自然人或特定群体因其年龄、残障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；

(c) 将此类人工智能系统投放市场、投入服务或加以使用，即根据自然人或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产生社会评分，导致以下任何一种或两种情况：

(i) 对特定自然人或群体产生有害或不利待遇，而这种待遇的社会场景与最初生成或收集数据的场景无关；

(ii) 对特定自然人或群体产生有害或不利待遇，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)投放市场、为了此类特定目的投入服务，或者使用此类人工智能系统，即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用户画像或对其个性特征和特点的评估；这一禁令不适用于用于支持人类评估某人参与犯罪活动的人工智能系统，如果某人已经具备与犯罪活动直接相关的客观和可验证的事实；

(e)投放市场、为了此类特定目的投入服务，或者使用此类人工智能系统，即通过从互联网或闭路电视录像中无区别地爬取面部图像来创建或扩展面部识别数据库；

(f) 投放市场、为了此类特定目的投入服务，或者使用此类人工智能系统，即在工作场所和教育机构领域推断自然人的情绪，但出于医疗或安全原因将人工智能系统投入服务或投放市场的情况除外；

(g) 投放市场、为了此类特定目的投入服务，或者加以使用生物分类系统，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或在执法领域对生物傻逼数据分类而对合法获取的生物识别数据集，如图像，进行标注或过滤。

(h) 在公众可进入的场所为执法目的使用“实时”远程生物识别系统，除非这种使用相应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最长刑期最长不少于四年的

监禁或拘留令。

本段第(h)项不影响(EU)2016/679 条例第 9 条关于非执法目的生物识别数据处理的规定。

2.根据第 1 段第 1 分段第(h)项的任何目标，而在公众可进入的场所为执法目的使用“实时”远程生物识别系统，只能用于该项所述的目的，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，为实现本条第 1 段第 1 分段第(h)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 27 条规定的基本权利影响评估，并根据第 49 条的规定在欧盟数据库中登记了该系统后，才可授权在公众可进入的场所使用“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.根据第 1 段第 1 分段第(h)项和第 2 段，每次在公众可进入的场所为执法目的使用“实时”远程生物识别系统时，应当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，并根据第 5 段的国家法律提出理由请求。然而，在紧急情况下，可以在没有授权的情况下开始使用此类系统，但应在不超过 24 小时内请求授权。如果授权被拒绝，应立即停止使用，并立即丢弃和删除所有数据、结果和输出。司法机关或具有约束力的独立行政机关应在基于提供的客观证据或明确指示满足第 1 段第(h)项所述目标的必要性和适当性，并特别确保时间、地理和人员范围的限制仅限于严格必要时才授予授权。该机关在决定请求时应考虑第 2 段所述的因素。不得仅基于“实时”远程生物识别系统的输出做出对个人产生不利法律效果的决定。

4.在不影响第 3 段的情况下，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 5 段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 6 段规定的信息，不得包括敏感业务数据。

5.成员国可在第 1 段第 1 分段第(h)项、第 2 段和第 3 段所列的限制和条件下，为执法目的，决定提供全部或部分授权在公众可进入的场所使用“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 段所述授权的申请、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 段第 1 分段第(h)项所列的目标中，包括第(h)项第 3 目所指的刑事犯罪，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 天内将其通知欧盟委员会。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。

6.成员国的国家市场监督管理机关和国家数据保护机关在收到第 4 段规定的在公众可以进入的场所中为执法目的使用“实时”远程生物识别系统的通知后，应向欧盟委员会提交关于此使用的年度报告。为此，欧盟委员会应向成员国和国家市场监督管理和数据保护机关提供模板，包括有关主管司法机关或其决定对根据第 3 款提出的授权请求具有约束力的独立行政机关

所作决定数目将其结果的信息。

7.欧盟委员会应根据成员国基于第 6 段所述年度报告的汇总数据，发布关于为执法目的在公众可以进入的场所使用“实时”远程生物识别系统的年度报告。这些年度报告不应包括相关执法活动的敏感业务数据。

8.本条款不影响其他欧盟法律规定的禁止人工智能实践的相关规定。

第三章

高风险人工智能系统

第一节
作为高风险人工智能系统的分类

第 6 条
高风险人工智能系统的分类规则

1. 无论人工智能系统是否独立于第(a)和(b)项所述产品被投放市场或投入服务，当以下条件被同时满足，该人工智能系统就应被视为高风险系统：
   (a) 人工智能系统被期望用作产品的安全部件，或者人工智能系统本身就是附件一所列欧盟统一立法所涵盖的产品；
   (b) 根据第(a)项其安全部件为人工智能系统的产品，或人工智能系统本身属于产品，则必须接受第三方合格性评估，以便根据附件一所列的欧盟统一立法将该产品投放市场或投入服务。

2. 除第 1 段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。

3. 根据对第 2 段的克减，附件三所指的人工智能系统如果不会对自然人的健康、安全或基本权利造成显著损害风险，包括不会对决策结果产生实质影响，则不应被视为高风险。

   第 1 分段适用于符合以下任何条件的情况：
   (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) 人工智能系统旨在执行与附件三所列用例有关的评估的准备任务。

尽管存在本段第一分段的规定，但如果附件三提及的人工智能系统对自然人进行用户画像，则该系统应始终被视为高风险系统。

4. 提供者认为附件三所述人工智能系统不是高风险系统，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 49 条第（2）段规定的登记义务。应成员国主管机关的要求，提供者应提供评估文件。

5. 欧盟委员会应在咨询欧盟人工智能委员会（以下简称"委员会"）后，在 2026 年 2 月 2 日之前，根据第 96 条的规定，提供具体实施本条的指南，以及一份人工智能系统高风险和非高风险用例的综合实例清单。

6. 欧盟委员会有权根据第 97 条通过授权法案，对本条第 3 段第 2 分段进行修订，在其中规定的条件之外增加新的条件，或对其进行修改，只要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，但不会对自然人的健康、安全或基本权利造成显著损害风险。

7. 欧盟委员会应根据第 97 条通过授权法案，通过删除其中规定的任何条件以修改本条第 3 段第 2 分段，如果有具体可靠的证据表明，这对保持本条例规定的健康、安全和基本权利的保护水平有必要。

8. 根据本条第 6 段和第 7 分段对第 3 段第 2 分段规定的条件所做的任何修改，不得降低本条例对健康、安全和基本权利的总体保护水平，并应确保与根据第 7(1) 条通过的授权法案保持一致，同时考虑到市场和技术的发展。

第 7 条
对附件三的修改

1. 欧盟委员会有权根据第 97 条通过授权法案，通过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，对附件三进行修正：
   (a) 拟在附件三所列的任何领域使用的人工智能系统；
   (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. 在评估第 1 段第（b）项规定的条件时，欧盟委员会应考虑以下标准：
   (a) 人工智能系统的预期目的；
   (b) 人工智能系统被使用或可能被使用的程度；
   (c) 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；
   (d) 人工智能系统自主行事的程度，以及人类推翻可能导致潜在伤害的决定或建议的可能性；
   (e) 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影响，或在多大程度上引起了对这种损害或不利影响的可能性的显著关切，例如，通过提交给成员国主管机关的报告或被记录的指控，或酌情提交的其他报告所证明的；
   (f) 这种损害或不利影响的潜在程度，特别是其严重性及其影响多人或对某一特定群体造成不成比例影响的能力；
   (g) 可能受到伤害或不利影响的人在多大程度上依赖于人工智能系统产生的结果，特别是因为出于实际或法律原因，对该结果不太可能合理地选择退出；
   (h) 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的部署者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；
   (i) 虑到现有的纠正或逆转的技术解决方案，人工智能系统产生的结果在多大程度上是容易纠正或逆转的；对健康、安全或基本权利有不利影响的结果不应被视为容易纠正或逆转的；

(j) 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；

(k) 现有欧盟法律在多大程度上规定了

(i) 与人工智能系统带来的风险有关的有效补救措施，但不包括损害赔偿主张；

(ii) 预防或实质减少这些风险的有效措施。

3. 当同时满足如下两个条件时，欧盟委员会有权根据第 97 条的规定通过授权法案，对附件三的清单进行修改：

(a) 考虑到第 2 段所列的标准，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) 此种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。

第二节
对高风险人工智能系统的要求

第 8 条
合规要求

1. 高风险人工智能系统应符合本节规定的要求，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。

2. 如果产品包含一个人工智能系统，而本条例的要求以及附件一 A 节所列欧盟统一立法的要求适用于该系统，则提供者应负责确保其产品完全符合适用的欧盟统一立法的所有适用要求。在确保第 1 段中提及的高风险人工智能系统符合本节规定的要求时，为了确保一致性、避免重复和最小化额外负担，提供者可选择酌情将其提供的有关其产品的必要测试和报告流程、信息和文件整合到附件一 A 节所列欧盟统一立法要求的已有文件和程序中。

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。它应包括以下步骤：

(a) 识别和分析高风险人工智能系统在按照其预期目的使用时可能对健康、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使用时，以及在可合理预见的滥用条件下可能出现的风险；

(c) 根据对从第 72 条提及的后市场监测系统中收集的数据的分析，评估可能出现的其他

风险；

(d) 采取适当的、有针对性的风险管理措施，以应对根据第(a)项确定的风险。

3. 本条所指的风险只涉及那些通过高风险人工智能系统的开发或设计，或提供充分的技术信息可以合理减轻或消除的风险。

4. 第 2 段第(d)项所述的风险管理措施应适当考虑本节所列各项要求的综合应用所产生的影响和可能的相互作用，以便更有效地把风险减少到最低限度，同时在实施满足这些要求的措施时取得适当的平衡。

5. 第 2 段第(d)项所指的风险管理措施，应使与每一危险相关的剩余风险以及高风险人工智能系统的总体剩余风险被判定为可以接受。

在确定最适当的风险管理措施时，应确保以下几点；

(a) 在技术可行的情况下，通过充分设计和开发高风险人工智能系统，消除或减少根据第 2 段确定和评估的风险；

(b) 针对无法消除的风险，酌情采取适当的缓解和控制措施；

(c) 提供第 13 条所要求的信息，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、预期的培训以及打算使用该系统的假定场景。

6. 对高风险人工智能系统应进行测试，以确定最合适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的运行符合其预期目的，并符合本节规定的要求。

7. 测试程序可包括根据第 60 条在真实世界条件下进行的测试。

8. 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，并在任何情况下在其投放市场或投入服务之前进行。测试应根据事先确定的指标和概率阈值进行，这些指标和阈值应与高风险人工智能系统的预期目的相适应。

9. 在实施第 1 至第 7 段规定的风险管理系统时，提供者应考虑到高风险人工智能系统的预期目的是否可能对 18 岁以下的人产生不利影响并且，并酌情考虑对其他弱势群体产生不利影响。

10. 对于根据欧盟法律其他相关规定须遵守内部风险管理流程要求的高风险人工智能系统提供者而言，第 1 至 9 段规定的方面可作为根据其他规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. 使用涉及用数据训练人工智能模型的技术的高风险人工智能系统，应在使用符合第 2 至第 5 段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与高风险人工智能系统预期目的相适应的数据治理和管理做法。

这些做法应特别注意：

(a) 相关的设计选择；
(b) 数据收集过程和数据来源，如果是个人数据，收集数据的最初目的；
(c) 相关的数据准备处理工作，如注释、标注、清洗、更新、充实和聚合；
(d) 假设的表达，特别是有关数据应衡量和代表的信息；
(e) 评估所需数据集的可得性、数量和适宜性；
(f) 检验可能会影响人员的健康和安全，对基本权利产生负面影响，或导致欧盟法律禁止的歧视的可能偏见，特别是在数据输出影响未来操作输入的情况下；
(g) 采取适当措施，发现、预防和减少根据第(f)项发现的可能的偏见；
(h) 识别妨碍遵守本条例的相关数据缺失或缺陷，以及如何解决这些缺失和缺陷。

3. 训练、验证和测试数据集应具有相关性、充分的代表性，并在最大程度的可能性上，从预期目的来看是无误且完整的。数据集应具有适当的统计特性，包括在适用的情况下，具有与打算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符合要求。

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打算使用的具体地理、场景、行为或功能环境所特有的特征或要素。

5. 在根据本条第 2 段第(f)和(g)项确保与高风险人工智能系统有关的偏见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特殊类别的个人数据，但须对自然人的基本权利和自由采取适当的保障措施。除(EU)第 2016/679 号和(EU)第 2018/1725 号条例以及(EU)第 2016/680 号指令中的规定外，必须满足以下所有条件才能进行此类处理：

(a) 通过处理其他数据，包括合成数据或匿名数据，无法有效实现偏见检测和纠正；
(b) 对特殊类别个人数据的再使用进行技术限制，并采取最先进的安全和隐私保护措施，包括假名化；
(c) 对特殊类别的个人数据采取措施，确保所处理的个人数据安全、受保护、有适当的保障措施，包括对访问的严格控制和记录，以避免滥用，并确保只有经授权的人员才能访问这些个人数据并承担适当的保密义务；
(d) 特殊类别的个人数据不得传输、转移或以其他方式被其他方获取；
(e) 一旦偏见得到纠正或个人数据的保存期结束，二者中的一个条件满足，特殊类别的个人数据即被删除；
(f) 根据(EU)2016/679 和(EU)2018/1725 条例以及(EU)2016/680 指令进行的处理活动记录，包括处理特殊类别个人数据对于发现和纠正偏见是绝对必要的原因，以及处理其他数据无法实现该目标的原因。

6. 对于不使用涉及人工智能模型训练技术的高风险人工智能系统的开发，第 2 至 5 段仅适用于测试数据集。

第 11 条
技术性文件

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节规定的要求，并能以清晰和全面的形式向成员国主管机关和被通知机构提供必要的信息，以评估人工智能系统是否符合这些要求。它至少应包括附件四所列的内容。中小企业，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，欧盟委员会将针对小型和微型企业的需要制定简化的技术文件格式。如果中小型企业，包括初创企业，选择以简化方式提供附件四所要求的信息，则应使用本段中提到的表格。被通知机构在进行合格性评估时应接受该表格。

2. 当与附件一 A 节所列欧盟统一立法所涵盖的产品有关的高风险人工智能系统投放市场或投入服务时，应制定一套单一的技术文件，其中包含第 1 段规定的所有信息，以及这些法案所要求的信息。

3. 欧盟委员会有权根据第 97 条通过授权法案，以便在必要时修改附件四，确保技术文件根据技术发展提供所有必要信息，以评估系统是否符合本节规定的要求。

第 12 条
记录保存

1. 高风险人工智能系统应在技术上允许自动记录系统整个生命周期发生的事件（日志）。

2. 为了确保高风险人工智能系统的运行具有与系统预期目的相适应的可追溯性，日志记录功能应能记录与以下方面相关的事件：
   (a) 确定可能导致高风险人工智能系统产生第 79 条第 1 段意义上的风险或导致实质性修改的情况；
   (b) 促进第 72 条所指的投放市场后的监测；以及
   (c) 监测第 26 条第 5 段所指的高风险人工智能系统的运行。

3. 对于附件三第 1(a)项所指的高风险人工智能系统，记录功能至少应包括：
   (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) 与搜索结果匹配的输入数据；
   (d) 如第 14 条第 5 段所述，参与核查结果的自然人的身份信息。

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，以遵守第 3 节中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，这些信息对部署者来说是相关的、可获取的和可理解的。

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）的身份和详细联系信息；
   (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 条所述的度量、稳健性和网络安全，以及可能对预期准确性水平、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. 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任何已知或可预见的可能导致第 9 条第 2 段所述健康与安全或基本权利风险的情况；
      iv. 在适用的情况下，高风险人工智能系统的技术能力和特点，以提供与解释其输出相关的信息；
      v. 在适当情况下，特定个体或群体预期使用该系统的性能；
      vi. 考虑到高风险人工智能系统的预期目的，酌情提供输入数据的说明，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；
      vii. 在适用的情况下，使部署者能够解释高风险人工智能系统的输出结果并加以适当使用的信息；
   (c) 提供者在初始符合性评估时预先确定的对高风险人工智能系统及其性能的改变，如果有的话；
   (d) 第 14 条所述的人类监督措施，包括为便于部署者解释高风险人工智能系统的输出而采取的技术措施；
   (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；
   (f) 在相关时，说明高风险人工智能系统所包含的机制，使部署者能够根据第 12 条适当收集、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，包括适当的人机界面工具，应使其在使用期间能由自然人进行有效监督。

2. 人类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照其预期目的使用或

在可合理预见的滥用条件下使用时可能出现的对健康、安全或基本权利的风险，特别是在尽管适用了本节规定的其他要求但这种风险依然存在的情况下。

3. 监督措施应与高风险人工智能系统的风险、自主程度和使用环境相称，并应通过以下一种或两种措施加以确保：
   (a) 在技术可行的情况下，在高风险人工智能系统投放市场或投入服务之前，由提供者确定并纳入该系统的措施；
   (b) 提供者在将高风险人工智能系统投放市场或投入服务之前确定的、适合由部署者实施的措施。

4. 为执行第 1、第 2 和第 3 段的目的，向部署者提供高风险人工智能系统的方式， 应使被指派进行人类监督的自然人能够在适当和相称的情况下：
   (a) 适当了解高风险人工智能系统的相关能力和局限性，并能够适当监测其运行情况，包括发现和处理异常情况、功能障碍和意外表现；
   (b) 意识到可能存在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（自动化偏见）的趋势，尤其是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) 正确解读高风险人工智能系统的输出结果，同时考虑到可用的解读工具和方法等；
   (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 1（a）项所述的高风险人工智能系统，本条第 3 段所述的措施应确保，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查和确认。

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。

2. 为解决如何衡量本条第 1 段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，欧盟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度量方法。

3. 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。

4. 对于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，特别是由于与自然人或其他系统的交互作用而出现的错误、故障或不一致，高风险人工智能系统应尽可能具有韧性。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。

在投放市场或投入服务后仍在继续学习的高风险人工智能系统，其开发方式应尽可能消除或减少可能有偏见的输出影响未来操作的输入（反馈回路）的风险，并确保任何此类反馈回路都能通过适当的缓解措施得到妥善处理。

5. 高风险人工智能系统应能够抵御未经授权的第三方通过利用系统漏洞改变其使用、输出或性能的企图。
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、解决和控制试图操纵训练数据集（“数据投毒”）或操纵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缺陷。

第三节
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章第二节的要求；
(b) 在高风险人工智能系统上标明其名称、登记商业名称或登记商标、可联系到其的地址，如无法标明，则在包装或随附文件上标明；
(c) 具有符合第 17 条规定的质量管理体系；
(d) 保存第 18 条提及的文件；
(e) 在其控制下保存第 19 条所述高风险人工智能系统自动生成的日志；
(f) 确保高风险人工智能系统在投放市场或投入服务之前经过第 43 条所述的相关合格性评估程序；
(g) 根据第 47 条的规定起草欧盟合格性声明；
(h) 根据第 48 条的规定，在高风险人工智能系统上加贴 CE 标志，或在无法加贴 CE 标志的情况下，在其包装或随附文件上加贴 CE 标志，以表明其符合本规定；
(i) 遵守第 49 条第 1 段所述的登记义务；
(j) 采取必要的纠正措施并提供第 20 条所要求的信息；
(k) 在成员国主管机关提出合理要求时，证明高风险人工智能系统符合第 2 节规定的要求；
(l) 确保高风险人工智能系统符合 (EU)2016/2102 和 2019/882 指令的无障碍要求。

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) 应采用的技术规范，包括标准，如果没有完全采用相关的统一标准，或没有涵盖第 2 节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服务前和为投放市场或投入服务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 72 条的规定，建立、实施和维护后市场监测系统；
   (i) 根据第 73 条报告严重事件的相关程序；
   (j) 处理与成员国主管机关、其他相关机构（包括提供或支持数据访问的机构）、被通知机构、其他运营者、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 段所述方面的实施应与提供者组织的规模相称。在任何情况下，提供者都应尊重确保其高风险人工智能系统符合本条例所需的严格程度和保护水平。

3. 高风险人工智能系统的提供者，如果根据相关的部门性欧盟法必须履行质量管理系统或同等职能的义务，则可以将第 1 段所列方面作为根据该法律质量管理系统的一部分。

4. 对于根据欧盟金融服务法须遵守内部治理、安排或流程要求的金融机构，除本条第 1 段第(g)、(h)和(i)项外，应通过遵守相关欧盟金融服务法的内部治理安排或流程规则来履行建立质量管理体系的义务。为此，应考虑第 40 条中提及的任何统一标准。

第 18 条
文件保存

1. 提供者应在高风险人工智能系统投放市场或投入使用后的 10 年内，将以下资料交由成员国主管机关保存：
   (a) 第 11 条所述的技术性文件；
   (b) 第 17 条所述质量管理系统的相关文件；

(c) 有关被通知机构批准的变更的文件，如适用；
(d) 被通知机构发布的决定和其他文件，如适用；
(e) 第 47 条提及的欧盟合格声明。

2. 对于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的情况，各成员国应确定第 1 段所述文件在该段所述期限内仍由成员国主管机关处置的条件。

3. 如果提供者是金融机构，其内部治理、安排或流程须遵守欧盟金融服务法的要求，则应将技术文件作为根据相关欧盟金融服务法保存的文件的一部分予以保存。

第 19 条
自动生成日志

1. 高风险人工智能系统的提供者应保存由其高风险人工智能系统自动生成的第 12 条第 1 段所述日志，如果这些日志在其控制范围内。在不影响适用的欧盟法或成员国法律的情况下，日志的保存期应与高风险人工智能系统的预期目的相适应，至少为六个月，除非适用的欧盟法或成员国法律另有规定，特别是关于保护个人数据的欧盟法。

2. 金融机构的提供者，如果其内部治理、安排或流程须符合欧盟金融服务法的要求，则应将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法保存的文件的一部分进行保存。

第 20 条
纠正行动和提供信息的义务

1. 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，酌情予以撤消、禁用或召回。他们应通知有关高风险人工智能系统的分销商，并酌情通知部署者、授权代表和进口商。

2. 如果高风险人工智能系统存在第 79 条第 1 段所指的风险，且提供者意识到该风险，则应立即与报告部署者（如适用）合作调查原因，并通知主管高风险人工智能系统的市场监督管理机构，以及（如适用）根据第 44 条为该高风险人工智能系统颁发证书的被通知机构，特别是通知不符合的性质以及所采取的任何相关纠正措施。

第 21 条
与主管机关的合作

1. 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第 2 节所列要求的所有必要信息和文件，其语言应为有关成员国所

表明的欧盟机构官方语言之一，易于该机关理解。

2. 在主管机关提出合理要求后，提供者还应在适用的情况下允许提出要求的主管机关查阅第 12 条第 1 段所述高风险人工智能系统自动生成的日志，但以这些日志在其控制范围内为限。

3. 主管机关根据本条获得的任何信息应按照第 78 条规定的保密义务处理。

第 22 条
高风险人工智能系统提供者的授权代表

1. 在欧盟市场上提供其高风险人工智能系统之前，在第三国设立的提供者应通过书面授权任命一名在欧盟设立的授权代表。

2. 提供者应使其授权代表能够执行从提供者处收到的授权书中规定的任务。

3. 授权代表人应执行提供者授权书中规定的任务。它应根据请求，以主管机关指定的欧盟机构官方语言之一，向市场监督管理机构提供一份授权副本。就本条例而言，授权书应授权授权代表执行以下任务：
   (a) 核查第 47 条所指的欧盟合格声明和第 11 条所指的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；
   (b) 在高风险人工智能系统投放市场或投入使用后的 10 年内，向主管机关和第 74 条第 10 段提及的国家机关或机构提供指定授权代表的提供者的详细联系信息、第 47 条提及的欧盟合格声明副本、技术文件以及（如适用）被通知机构签发的证书；
   (c) 应主管机关的合理要求，提供所有必要的信息和文件，包括本分段(b)项所指的信息和文件，以证明高风险人工智能系统符合第 2 节规定的要求，包括查阅第 12 条第 1 段所指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；
   (d) 在主管机关采取的与高风险人工智能系统有关的任何行动中，特别是在减少和降低高风险人工智能系统造成的风险方面，应主管机关的合理要求与之合作；
   (e) 在适用的情况下，遵守第 49 条第 1 段所述的登记义务，如果登记是由提供者自己进行 的，则应确保附件八 A 节第 3 项所述的信息正确无误。

授权书应授权授权代表人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，接受主管机关的处理。

第 23 条
进口商的义务

1. 在将高风险人工智能系统投放市场之前，进口商应确保该系统符合本条例的规定，为此

应核查：

(a) 高风险人工智能系统的提供者已进行了第 43 条所述的相关合格评定程序；

(b) 提供者已根据第 11 条和附件四编制了技术文件；

(c) 系统带有所需的 CE 标志，并附有第 47 条所指的欧盟合格声明和使用说明；

(d) 提供者已根据第 22 条第 1 段的规定任命了授权代表。

2. 如果进口商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，或者是伪造的，或者附有伪造的文件，则在该系统符合规定之前不得将其投放市场。如果高风险人工智能系统存在第 79 条第 1 段所指的风险，进口商应将此情况通知系统提供者、授权代表和市场监督管理机构。

3. 进口商应在高风险人工智能系统及其包装或随附文件（如适用）上标明其名称、注册商号或注册商标以及联系地址。

4. 进口商应确保高风险人工智能系统由其负责时，储存或运输条件（如适用）不会危及其符合第 2 节规定的要求。

5. 进口商应在高风险人工智能系统投放市场或投入使用后的 10 年内，保存一份由被通知机构颁发的证书（如适用）、使用说明和第 47 条所述欧盟合格声明的副本。

6. 进口商应在有关主管机关提出合理要求后，以其易于理解的语言向其提供所有必要的信息和文件，包括第 5 段中提及的信息和文件，以证明高风险人工智能系统符合第 2 节中规定的要求。为此，还应确保向这些机关提供技术文件。

7. 进口商应与有关主管机关合作，配合主管机关对进口商投放市场的高风险人工智能系统采取任何行动，特别是减少和降低该系统构成的风险。

第 24 条
分销商的义务

1. 在市场上提供高风险人工智能系统之前，分销商应核查该系统是否带有所需的 CE 标志，是否附有第 47 条所述的欧盟合格声明副本和使用说明，以及该系统的提供者和进口商（如适用）是否遵守了第 16 条第(b)和(c)项以及第 23 条第 3 段规定的各自义务。
2. 如果分销商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第 2 节规定的要求，在该系统符合这些要求之前，分销商不得在市场上提供高风险人工智能系统。此外，如果高风险人工智能系统存在第 79 条第 1 段所指的风险，分销商应酌情将此情况通知该系统的提供者或进口商。

3. 分销商应确保在其负责高风险人工智能系统时，储存或运输条件（如适用）不会危及该系统符合第 2 节规定的要求。

4. 分销商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第 2 节所列要求，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、进口商或任何有关运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 79 条第 1 段所指的风险，分销商应立即通知该系统的提供者或进口商以及有关高风险人工智能系统的主管机关，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. 在有关主管机关提出合理要求后，高风险人工智能系统的分销商应向该主管机关提供有关其根据第 1 至第 4 段采取的行动的所有必要信息和文件，以证明该系统符合第 2 节规定的要求。
6. 分销商应与有关主管机关合作，采取任何与分销商在市场上提供的高风险人工智能系统有关的行动，特别是减少或降低该系统带来的风险。

第 25 条
人工智能价值链上的责任

1. 为本条例之目的，任何分销商、进口商、部署者或其他第三方应被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，应承担第 16 条规定的提供者义务：
   (a) 在已投放市场或投入服务的高风险人工智能系统上冠以自己的名称或商标，但不妨碍以其他方式分配义务的合同安排；
   (b) 对已投放市场或已投入服务的高风险人工智能系统进行重大修改，使其仍属于第 6 条所指的高风险人工智能系统；
   (c) 对未被列为高风险并已投放市场或投入服务的人工智能系统（包括通用人工智能系统）的预期目的进行修改，使有关人工智能系统根据第 6 条成为高风险人工智能系统。

2. 如果出现第 1 段所述情况，最初将人工智能系统投放市场或投入服务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。最初的提供者应与新的提供者密切合作，提供必要的信息，并提供合理预期的技术准入和为履行本条例规定义务所要求的其他协助，特别是关于遵守高风险人工智能系统合格性评估的义务。本段不适用于初始提供者已明确说明其人工智能系统不会被改变为高风险人工智能系统，因此不属于移交文件的义务范围的情况。

3. 如果高风险人工智能系统是附件一 A 部分所列欧盟统一立法所涵盖产品的安全部件，则产品制造商应被视为高风险人工智能系统的提供者，在下列任一情况下，应履行第 16 条规定的义务：
   (a) 高风险人工智能系统与产品制造商的名称或商标的产品一起投放市场；
   (b) 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服务。

4. 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充分遵守本条例规定的义务。本段不适用于在免费和开源许可下向公众提供工具、服务、流程或组件（通用人工智能模型除外）的第三方。

人工智能办公室可为高风险人工智能系统的提供者与提供用于高风险人工智能系统或集成到高风险人工智能系统的工具、服务、组件或流程的第三方之间的合同制定和推荐自愿示范条款。在制定这些自愿性示范条款时，人工智能办公室应考虑到适用于特定部门或商业案例的可能合同要求。自愿性示范条款应以易于使用的电子格式公布并免费提供。

5. 第 2 段和第 3 段不影响根据欧盟法律和国家法律遵守和保护知识产权、商业机密信息和商业秘密的需要。

第 26 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，确保按照第 3 段和第 6 段的规定，根据系统所附的使用说明使用这些系统；

2. 部署者应指派具备必要能力、培训和权威以及必要支持的自然人进行人工监督；

3. 第 1 段和第 2 段规定的义务不影响欧盟或国内法规定的其他部署者义务，也不影响部署者为执行提供者所述的人类监督措施而组织自身资源和活动的自由。

4. 在不影响第 1 段和第 2 段的情况下，只要部署者对输入数据行使控制权，就高风险人工智能系统的预期目的而言，部署者应确保输入数据具有相关性和充分代表性。

5. 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，并在相关情况下根据第 72 条通知提供者。如果部署者有理由认为，按照使用说明使用高风险人工智能系统可能导致该人工智能系统出现第 79 条第 1 段所指的风险，他们应在没有不当拖延的情况下通知提供者或分销商和有关市场监管管理机构，并应暂停使用该系统。如果部署者发现了严重事故，也应立即首先通知提供者，然后通知进口商或分销商以及事故相关的市场监管管理机构。如果部署者无法联系到提供者，则应比照适用第 73 条。这项义务不包括作为执法机关的人工智能系统部署者的敏感业务数据。
   对于根据欧盟金融服务法须遵守内部治理、安排或流程要求的金融机构部署者而言，遵守相关金融服务法规定的内部治理安排、流程和机制规则，即视为履行了第一分段规定的监控义务。

6. 高风险人工智能系统的部署者应在其控制范围内保存该高风险人工智能系统自动生成的日志，保存期应与高风险人工智能系统的预期目的相称，至少六个月，除非适用的欧盟或国家法律，特别是关于保护个人数据的欧盟法律另有规定。
   如果部署者是金融机构，其内部治理、安排或流程须遵守欧盟金融服务法的要求，则应将日志作为根据相关欧盟金融服务法保存的文件的一部分进行保存。

7. 在工作场所投入服务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劳动者代表和受影响的劳动者，他们将使用高风险人工智能系统。在适用的情况下，应根据欧盟和国家关于劳动者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。

8. 高风险人工智能系统的部署者如果是公共机关或欧盟机构、机关、办事处或机构，则应遵守第 49 条所述的登记义务。当这些部署者发现他们打算使用的高风险人工智能系统尚未在第 71 条所述的欧盟数据库中注册时，他们不得使用该系统，并应通知供应者或分销商。
9. 在适用的情况下，高风险人工智能系统的部署者应使用根据本条例第 13 条提供的信息，以履行其根据(EU)第 2016/679 号条例第 35 条或(EU)第 2016/680 号指令第 27 条进行数据保护影响评估的义务。

10. 在不影响第(EU)2016/680 号指令的情况下，在对涉嫌或被判定犯有刑事罪的人进行定向搜查的调查框架内，用于后远程生物特征识别的高风险人工智能系统的部署者应事先或在不无故拖延的情况下，在不迟于 48 小时内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，但根据与罪行直接相关的客观和可核查的事实初步识别潜在嫌疑人的情况除外。每次使用应仅限于调查特定刑事犯罪所严格需要的范围。

如果根据本段第一分段申请的授权被拒绝，则应立即停止使用与申请授权相关联的后远程生物识别系统，并删除与使用申请授权的高风险人工智能系统相关联的个人数据。

在任何情况下，这种用于后远程生物识别的高风险人工智能系统都不得用于无目标性的、与刑事犯罪、刑事诉讼、真正的和当前的或真正的和可预见的刑事犯罪威胁或寻找具体的失踪人员没有任何联系的执法。应确保执法机关不得仅根据这种后远程生物识别系统的输出结果作出对个人产生不利法律影响的决定。

本段不影响关于生物识别数据处理的(EU)第 2016/679 号条例第 9 条和(EU)第 2016/680 号指令第 10 条。
无论目的或部署者如何，此类高风险人工智能系统的每次使用都应记录在相关警方档案中，并应根据要求提供给相关市场监督机构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。本分段不得损害(EU)第 2016/680 号指令赋予监管机关的权力。
部署者应向有关市场监督管理机构和国家数据保护机构提交年度报告，说明其使用后远程生物识别系统的情况，但不包括披露与执法有关的敏感业务数据。报告可以汇总，以涵盖一个以上的部署情况。

成员国可根据欧盟法律，就后远程生物识别系统的使用制定限制性更强的法律。

11. 在不影响本条例第 50 条的情况下，附件三中提及的高风险人工智能系统的部署者在做出与自然人有关的决定或协助做出与自然人有关的决定时，应告知自然人他们是高风险人工智能系统的使用对象。对于用于执法目的的高风险人工智能系统，应适用(EU)第 2016/680 号指令第 13 条。

12. 部署者应在相关主管机关为执行本条例而对高风险人工智能系统采取的任何行动中与这些主管机关合作。

第 27 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 段所指的高风险人工智能系统之前，除了打算用于附件三第 2 项所列领域的高风险人工智能系统外，受公法管辖的机构或提供公共服务的私营实体以及附件三第 5(b)和(c)项所指的高风险人工智能系统的部署者，应评估使用这种系统可能对基本权利产生的影响。为此，部署者应进行包括以下内容的评估:
   (a) 说明部署者按照预期目的使用高风险人工智能系统的程序；
   (b) 说明打算使用每个高风险人工智能系统的期限和频率；
   (c) 在特定情况下使用该系统可能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，可能对根据本段(c)项确定的各类自然人或群体产生影响的具体危害风险；
   (e) 根据使用说明，说明人工监督措施的实施情况；
   (f) 在出现这些风险时应采取的措施，包括内部治理和投诉机制的安排。

2. 第 1 段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 段所列的任何要素已发生变化或不再是最新的，部署者应采取必要步骤更新信息。

3. 一旦进行了本条第 1 段所述的评估，部署者应将评估结果通知市场监督管理机构，并提交本条第 5 段所述的填写模板作为通知的一部分。在第 46 条第 1 段所述情况下，部署者可免除通知义务。

4. 如果本条规定的任何义务已通过根据(EU)第 2016/679 号条例第 35 条或(EU)第 2016/680 号指令第 27 条进行的数据保护影响评估得到履行，则本条第 1 段所述基本权利影响评估应作为该数据保护影响评估的补充。

5. 人工智能办公室应开发一个问卷模板，包括通过一个自动化工具，以方便部署者以简化的方式遵守本条规定的义务。

第 4 节
通知机关和被通知机构

第 28 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其监督的必要程序。这些程序应由所有成员国的通知机关合作制定。

2. 成员国可决定第 1 段所述的评估和监督工作由(EC)第 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其与合格性评估机构之间不存在利益冲突，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中进行评估的主管人员作出。

5. 通知机关不得提议或提供合格性评估机构从事的任何活动；也不得提供任何商业或竞争基础上的咨询服务。

6. 通知机关应根据第 78 条的规定，对其获得的信息进行保密。

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。主管人员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 29 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能胜任的人工智能系统类型的说明，以及由国家认证机构颁发的认证证书（如有），证明合格性评估机构符合第 31 条规定的要求。
与任何其他欧盟统一立法下的被通知机构申请者的现有名称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不能提供认证证书，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 31 条规定的要求进行核查、认可和定期监督。

4. 对于根据任何其他欧盟统一立法指定的被通知机构，与这些指定相关的所有文件和证书可酌情用于支持其根据本条例进行的指定程序。每当发生相关变化时，被通知机构应更新本条第 2 段和第 3 段提及的文件，以使负责被通知机构的机关能够监测和核查对第 31 条规定的所有要求的持续遵守情况。

第 30 条

通知程序

1. 通知机关只能通知符合第 31 条规定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 段中提及的每个合格性评估机构通知欧盟委员会和其他成员国。

3. 本条第 2 段提及的通知应包括合格性评估活动、合格性评估模块、有关人工智能系统的类型以及相关能力证明的全部细节。如果通知不是基于第 29 条第 2 段所述的认证证书，通知机关应向欧盟委员会和其他成员国提供文件证据，证明合格性评估机构的能力，以及为确保该机构定期接受监督并继续满足第 31 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欧盟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的情况下，并且通知机关的通知中包括第 29 条第 2 段所述的认可证书，或在被通知机构发出通知后两个月内包括第 29 条第 3 段所述的书面证据，方可开展被通知机构的活动。

5. 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，欧盟委员会应决定授权是否合理。欧盟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 31 条
与被通知机构有关的要求

1. 被通知机构应根据成员国的国内法成立，并应具有法人资格。

2. 被通知机构应满足完成其任务所必需的组织、质量管理、资源和流程要求，以及适当的网络安全要求。

3. 被通知机构的组织结构、职责分配、报告关系和运作应确保对其绩效和被通知机构开展的合格性评估活动的结果有信心。

4. 被通知机构应独立于与之开展合格性评估活动的高风险人工智能系统的提供者。被通知机构也应独立于在所评估的高风险人工智能系统中拥有经济利益的任何其他操作方，以及提供者的任何竞争对手。这并不排除为合格性评估机构的业务所必需的被评估的高风险人工智能系统的使用，也不排除为个人目的使用这些高风险人工智能系统。

5. 合格性评估机构、其高层管理人员、负责执行合格性评估任务的人员，都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。他们不得从事任何可能有损于其独立判断力或与其所负责的合格性评估活动有关的正直性的活动。这尤其适用于咨询服务。
6. 被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。被通知机构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。
7. 被通知机构应制定成文的程序，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 78 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，除非法律要求披露这些信息。被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。

8. 被通知机构应制定开展活动的程序，这些程序应适当考虑到提供者的规模、所处行业、

结构以及有关人工智能系统的复杂程度。

9. 被通知机构应为其合格性评估活动投保适当的责任险，除非责任由其根据国内法设立的成员国承担，或该成员国本身直接负责合格性评估。

10. 被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规定的所有任务，无论这些任务是由被通知机构自己执行，还是代表被通知机构和在他们的责任范围内执行。

11. 被通知机构应具备足够的内部能力，以便能够有效地评估由外部各方代表其执行的任务。被通知机构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，以及与第 2 节所列要求有关的经验和知识。

12. 被通知机构应参与第 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，或确保了解相关标准的最新情况。

第 32 条
与被通知机构有关的推定符合要求

如果合格性评估机构证明其符合相关统一标准或其部分规定的标准，而这些标准的参考资料已在《欧盟官方公报》上公布，则应推定该机构符合第 31 条规定的要求，只要适用的统一标准涵盖了这些要求。

第 33 条
被通知机构的附属机构和分包

1. 如果被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 31 条规定的要求，并应通知相应通知机关。

2. 被通知机构应对任何分包商或附属机构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，才能将活动分包或由子公司执行。被通知机构应公布其子公司名单。

4. 分包商或子公司资格评估的相关文件以及他们根据本条例开展的工作应由通知机关保存，保存期自分包终止之日起为期五年。

第 34 条
被通知机构的业务性义务

1. 被通知机构应按照第 43 条规定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. 被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，并应适当考虑提供者的规模、所处行业、结构和有关高风险人工智能系统的复杂程度，特别是考虑到要尽量减少 2003/361/EC 号建议书所指的微型和小型企业的行政负担和合规成本。尽管如此，被通知机构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。

3. 被通知机构应向第 28 条所述的通知机关提供并按要求提交所有相关文件，包括提供者的文件，以便该机构开展评估、指定、通知和监测活动，并为本节所述的评估提供便利。

第 35 条
根据本条例指定的被通知机构的识别号和名单

1. 欧盟委员会应为每个被通知机构分配一个单一的标识号，即使一个机构根据不止一个欧盟法案成为被通知机构。

2. 欧盟委应公布根据本条例通知的机构名单，包括其标识号及其被通知的活动。欧盟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 30 条第 2 段提及的电子通知工具，将对被通知机构通知的任何相关变更通知欧盟委员会和其他成员国。

2. 第 29 条和第 30 条规定的程序适用于通知范围的扩展。
对于除扩大范围以外的通知变更，应适用第 3 至 9 段规定的程序。

3. 如果被通知机构决定停止其合格性评估活动，它应尽快通知通知机关和有关提供者，如果是有计划的停止，至少应在停止活动前一年通知。在被通知机构停止活动后的九个月内，如果另一个被通知机构以书面形式确认它将承担这些证书所涵盖的高风险人工智能系统的责任，则被通知机构的证书可以继续有效。后一被通知机构应在九个月期限结束前完成对受影响的高风险人工智能系统的全面评估，然后再为这些系统签发新证书。如果被通知机构已停止活动，通知机关应撤销指定。

4. 如果通知机关有充分理由认为被通知机构不再符合第 31 条规定的要求，或认为它未能履行其义务，通知机关应立即尽最大努力调查此事。在这种情况下，它应将提出的反对意见通知有关被通知机构，并使其有可能发表意见。如果通知机关得出结论认为，被通知机构不再符合第 31 条规定的要求，或未能履行其义务，则应根据未能满足这些要求或履行这些义务的严重程度，酌情限制、中止或撤销指定。它应立即向欧盟委员会和其他成员国通报有关情况。

5. 如果其指定已被中止、限制或全部或部分撤销，被通知机构应在 10 天内通知有关提供者。

6. 在限制、中止或撤销指定的情况下，通知机关应采取适当步骤，确保保存有关被通知机构的档案，并应其他成员国的通知机关和市场监督管理机构的要求向其提供这些档案。

7. 在限制、中止或撤销指定的情况下，通知机关应：
   (a) 评估对被通知机构签发的证书的影响；
   (b) 在通知更改指定后的三个月内，向欧盟委员会和其他成员国提交一份关于其评估结果的报告；
   (c) 要求被通知机构在主管机关确定的合理期限内，中止或收回任何不当签发的证书，以确保市场上的高风险人工智能系统继续符合要求；
   (d) 向欧盟委员会和成员国通报其要求中止或撤销的证书；
   (e) 向提供者注册营业地所在成员国的成员国主管机关提供其要求中止或撤销的证书的所有相关信息；该主管机关应在必要时采取适当措施，以避免对健康、安全或基本权利造成潜在风险。

8. 除不当签发的证书外，在指定被中止或限制的情况下，证书在下列任一情况下继续有效：
   (a) 通知机关在暂停或限制后一个月内确认，受暂停或限制影响的证书不存在危及健康、安全或基本权利的风险，且通知机关概述了补救中止或限制的行动时间表；或
   (b) 通知机关已确认在暂停或限制期间不会签发、修改或重新签发与中止有关的证书，并说明被通知机构是否有能力在暂停或限制期间继续监督和负责已签发的现有证书；如果通知机关确定该被通知机构没有能力支持已签发的现有证书，则证书所涉系统的提供者应在中止或限制的三个月内，以书面形式向其注册营业地所在成员国的成员国主管机关确认，在中止或限制期间，另一个合格的被通知机构将临时承担被通知机构的职能，对证书进行监督并继续负责。

9. 在下列情况下，证书的有效期应为九个月，但不当发放的证书和已撤销的指定除外：
   (a) 证书所涵盖的高风险人工智能系统的提供者的注册营业地所在的成员国的成员国主管机关已确认，有关的高风险人工智能系统对健康、安全或基本权利没有风险；以及
   (b) 另一被通知机构已书面确认将立即对这些人工智能系统负责，并在撤销指定后 12 个月内完成评估。

在第一项所述情况下，证书所涉系统的提供者营业地所在成员国的成员国主管机关可将证书的临时有效期再延长三个月，但总共不得超过 12 个月。

成员国主管机关或承担受指定变更影响的被通知机构职能的被通知机构应立即将此事通知欧盟委员会、其他成员国和其他被通知机构。

第 37 条
对被通知机构能力的质疑

1. 必要时，欧盟委员会应调查所有有理由怀疑被通知机构能力或被通知机构是否继续履行第 31 条规定的要求及其适用责任的情况。

2. 当欧盟委员会提供要求，通知机关应提供与通知有关或保持该被通知机构能力有关的所有相关信息。

3. 欧盟委员会应确保在根据本条进行调查的过程中获得的所有敏感信息均按照第 78 条的规定予以保密。

4. 当欧盟委员会确定某一被通知机构不符合或不再符合其通知要求时，应将此情况通知实施通知的成员国，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，欧盟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 98 条第 2 段所述的审查程序通过。

第 38 条
被通知机构的协调

1. 对于高风险人工智能系统，欧盟委员会应确保在根据本条例开展合格性评估程序的被通知机构之间建立适当的协调与合作，并以被通知机构部门小组的形式适当运作。

2. 各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第 1 段所述小组的工作。

3. 欧盟委员会应规定各通知机关之间知识交流和最佳实践。

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的法律建立的合格性评估机构，只要符合第 31 条规定的要求或确保同等水平的合规性，即可被授权开展本条例规定的被通知机构活动。

第 5 节
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

1. 高风险人工智能系统或通用人工智能模型，如符合《欧盟官方公报》根据(EU)第 1025/2012 号条例公布的统一标准或其部分内容，应推定为符合本章第 2 节规定的要求，或在适用情况下，符合本条例第五章第 2 节和第 3 节规定的义务，只要这些标准涵盖了这些要求或义务。

2. 根据(EU)第 1025/2012 号条例第 10 条，欧盟委员会应在不无故拖延的情况下，发出涵盖本章第 2 节所列所有必要条件的标准化要求，并在适用的情况下，发出涵盖本条例第五章第 2 节和第 3 节所列义务的标准化要求。标准化申请还应要求提供有关报告和文件流程的交付成果，以改善人工智能系统的资源性能，例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。在准备标准化申请时，欧盟委员会应咨询委员会和相关利益方，包括咨询论坛。

在向欧洲标准化组织发出标准化请求时，欧盟委员会应明确规定，标准必须清晰、一致，包括与附件一所列欧盟现有统一立法所涵盖产品的各部门制定的标准一致，并旨在确保在欧盟市场上投放或投入使用的高风险人工智能系统或通用人工智能模型符合本条例规定的相关要求或义务。

欧盟委员会应要求欧洲标准化组织提供证据，证明其根据(EU)第 1025/2012 号条例第 24 条的规定，为实现本段第一和第二项所述目标而做出的最大努力。

3. 标准化进程的参与者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，以及欧盟市场的竞争力和增长，为加强全球标准化合作做出贡献，并考虑到人工智能领域符合欧盟价值观、基本权利和利益的现有国际标准，加强多方利益相关者治理，确保利益的均衡代表和所有相关利益相关者根据(EU)第 1025/2012 号条例第 5、6 和 7 条的规定有效参与。

第 41 条
共同规格

1. 在满足以下条件的情况下，欧盟委员会可通过实施法案，为本章第 2 节规定的要求，或在适用的情形下为第 5 章第 2 节和第 3 节规定的义务制定共同规格：

(a) 根据(EU)第 1025/2012 号条例第 10 条第 1 段，欧盟委员会要求一个或多个欧洲标准化组织为本章第 2 节所列要求或（如适用）第五章第 2 和第 3 节所列义务起草统一标准，且
   i. 该请求未被任何一个欧洲标准化组织接受；或
   ii. 处理该请求的统一标准未在根据(EU)第 1025/2012 号条例第 10(1) 条规定的最后期限内交付；或
   iii. 相关统一标准未充分解决基本权利问题；或
   iv. 统一标准不符合要求；且

(b) 根据第欧盟 1025/2012 号条例，《欧盟官方公报》未公布涉及本章第 2 节所述要求或第 5 章第 2 节和第 3 节所述义务（如适用）的统一标准参考，且预计在合理期限内不会公布此类参考。

在起草共同规格时，欧盟委员会应咨询第 67 条所指的咨询论坛。

本段第 1 分段提及的实施法案应根据第 98 条第 2 段提及的审查程序通过。

2. 在起草实施法案草案之前，欧盟委员会应告知(EU)第 1025/2012 号条例第 22 条所述的委员会，欧盟委员会认为本条第 1 段规定的条件已经满足。
3. 高风险人工智能系统或通用人工智能模型，如符合第 1 段所述共同规格或部分规格，

则应推定为符合本章第 2 节所列要求，或在适用情况下，符合第五章第 2 节和第 3 节所述义务，只要这些共同规格涵盖这些要求或义务。

4. 当欧洲标准化组织通过一项统一标准，并建议欧盟委员会在《欧盟官方公报》上公布其参照时，欧盟委员会应根据(EU)第 1025/2012 号条例对该统一标准进行评估。在《欧盟官方公报》上公布统一标准的参照时，欧盟委员会应废除第 1 段中提及的实施法案，或其中涉及本章第 2 节规定的相同要求，或在适用的情况下的第 5 章第 2 节和第 3 节规定的相同义务部分。

5. 如果高风险人工智能系统或通用人工智能模型的提供者不符合第 1 段所述共同规格，则应充分说明其采用的技术解决方案符合本章第 2 节所述要求，或在适用情况下，符合第五章第 2 节和第 3 节规定的义务，至少达到与之相当的水平。

6. 如果成员国认为共同规格不完全符合本章第 2 节的要求，或在适用情况下不符合第 5 章第 2 节和第 3 节规定的义务，则应将此情况通知欧盟委员会并做出详细解释。欧盟委员会应评估该信息，并酌情修订确立相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、背景或功能环境，则应推定该系统符合第 10 条第 4 段规定的相关要求。

2. 根据(EU)第 2019/881 号条例，高风险人工智能系统如已获得认证或已根据网络安全计划发布合格声明，且其参考已在《欧盟官方公报》上公布，则应推定其符合本条例第 15 条规定的网络安全要求，只要网络安全证书或合格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 项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第 2 节所列要求时，提供者采用了第 40 条所指的统一标准，或在适用的情况下采用了第 41 条所指的共同规格，提供者应选择以下一种合格评定程序，其依据是：

(a) 附件六所述的内部控制；或

(b) 附件七所述的有被通知机构参与的质量管理体系评估和技术文件评估。

如果存在下述情况，在证明高风险人工合成系统符合第 2 节所列要求时，提供者应遵循附件七所列的合格性评估程序：

(a) 不存在第 40 条所述的统一标准，也不存在第 41 条所述的共同规格；

(b) 提供者未应用或仅应用了部分统一标准；

(c) 存在第(a)项所述的共同规格，但提供者没有采用；

(d) 第(a)项中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，提供者可以选择任何一个被通知机构。但是，如果高

风险人工智能系统打算由执法、移民或庇护机关或欧盟机构、机关、办事处或机构投入使用，则第 74 条第 8 段或第 9 段所述的市场监督管理机构在适当的情况下应充当被通知机构。

2. 对于附件三第 2 至第 8 项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评定程序，该程序没有规定被通知机构的参与。

3. 对于附件一 A 节所列欧盟统一立法所涵盖的高风险人工智能系统，提供者应遵循这些法案所要求的相关符合性评定程序。本章第 2 节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 项和第 4.6 项第 5 段也应适用。

为评估之目的，已根据这些法案获得通知的被通知机构应有权控制高风险人工智能系统是否符合第 2 节规定的要求，前提是这些被通知机构已根据这些法案的通知程序评估了是否符合第 31 条第 4、5、10 和 11 段规定的要求。

如果附件一 A 节所列的某项法案允许产品制造商选择不参加第三方合格性评估，条件是该制造商已采用了涵盖所有相关要求的所有统一标准，则该制造商只有在也采用了涵盖本章第 2 节所列所有要求的统一标准，或在适用条件下采用了第 41 条所提及的共同规格时，才可使用该选择。

4. 已经接受过合格性评估程序的高风险人工智能系统，在进行重大修改时，无论修改后的系统是打算进一步分销还是由目前的部署者继续使用，都应接受新的合格性评估程序。

对于在投放市场或投入服务后继续学习的高风险人工智能系统，如果对高风险人工智能系统及其性能的修改是由提供者在首次合格性评估时预先确定的，并且是附件四第 2 条第(f)项所述技术性文件所载信息的一部分，则不构成实质性修改。

5. 欧盟委员会有权根据第 97 条的规定通过授权法案，以便根据技术发展对附件六和七进行修订。

6. 欧盟委员会有权根据第 97 条通过授权法案，对本条第 1 段和第 2 段进行修改，以使附件三第 2 至第 8 项中提及的高风险人工智能系统接受附件七中提及的合格性评估程序或部分程序。欧盟委员会在通过这些授权法案时，应考虑到附件六所述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，以及被通知机构是否具备足够的能力和资源。

第 44 条
认证

1. 被通知机构根据附件七签发的证书，其语言应便于被通知机构所在成员国的有关机关理解。

2. 证书的有效期为：附件一所涵盖的人工智能系统不超过五年，附件三所涵盖的人工智能系统不超过四年。应提供者的要求，证书的有效期可根据按照适用的合格性评估程序进行的重新评估予以延长，对附件一所列的人工智能系统而言，每次延长不得超过五年，对附件三所列的人工智能系统而言，每次延长不得超过四年。只要证书是有效的，那么对证书的任何补充应继续有效。

3. 如果被通知机构发现某个人工智能系统不再符合第 2 节所列的要求，它应在考虑到相称性原则的情况下，暂停或收回所签发的证书或对其施加限制，除非该系统的提供者在被通知机构规定的适当期限内采取了适当的纠正措施以确保符合这些要求。被通知机构应说明其决定的理由。对被通知机构的决定，包括对颁发的合格证书的决定，应有申诉程序。

第 45 条
被通知机构的信息义务

1. 被通知机构应向通知机关通报以下内容：
(a) 任何欧盟技术文件评估证书、对这些证书的任何补充，以及根据附件七的要求颁发的任何质量管理体系批准；
(b) 任何拒绝、限制、暂停或撤销欧盟技术性文件评估证书，或根据附件七的要求颁发的质量管理体系批准书的情况；
(c) 任何影响通知范围或通知条件的情况；
(d) 从市场监督管理机构收到的关于提供合格性评估活动信息的任何要求；
(e) 应要求提供在其申报范围内开展的合格性评估活动和开展的任何其他活动，包括跨境活动和分包活动。

2. 每个被通知机构应将以下情况通知其他被通知机构：
(a) 其已拒绝、暂停或撤销的质量管理体系批准，以及应要求其已颁发的质量体系批准；
(b) 其已拒绝、撤回、暂停或以其他方式限制的欧盟技术性文件评估证书或其任何补充，并应要求提供其已颁发的证书和/或补充。

3. 每个被通知机构应向其他开展类似合格性评估活动的被通知机构提供涉及相同类型人工智能系统的负面合格性评估结果的相关信息，并应要求提供正面合格性评估结果的相关信息。

4. 被通知机构应根据第 78 条的规定对其获得的信息保密。

第 46 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构均可出于公共安全或保护人的生命和健康、环境保护或保护关键工业和基础设施资产的特殊原因，授权在有关成员国境内将特定的高风险人工智能系统投放市场或投入服务。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。

2. 在因公共安全的特殊原因而有正当理由的紧急情况下，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以不经第 1 段所述授权而将特定的高风险人工智能系统投入服务，前提是在使用过程中或使用之后申请这种授权，不得无故拖延。如果第 1 段所述授权遭到拒绝，则应立即停止使用高风险

人工智能系统，并应立即丢弃使用该系统的所有结果和产出。

3. 只有当市场监督管理机构认定高风险人工智能系统符合第 2 节的要求时，才可签发第 1 段所述授权。市场监管机构应将根据第 1 段和第 2 段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操作数据。

4. 如果在收到第 3 段所述信息后 15 个自然日内，成员国或欧盟委员会均未对成员国市场监督管理机构根据第 1 段发出的授权提出异议，则该授权应被视为合理。

5. 如果在收到第 3 段所述通知后 15 个自然日内，一成员国对另一成员国市场监督管理机构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 3 段所述系统合规性的结论没有根据，欧盟委员会应立刻与相关成员国进行磋商。应征求有关运营者的意见，并使其有可能提出自己的看法。在考虑了这些意见后，欧盟委员会应决定授权是否合理。欧盟委员会应将其决定通知有关成员国和相关操作方。

6. 如果欧盟委员会认为授权不合理，有关成员国的市场监管机构应撤销授权。

7. 对于与附件一 A 部分所列欧盟统一立法涵盖的产品有关的高风险人工智能系统，仅适用该欧盟统一立法中规定的合格性评估的克减。

第 47 条
欧盟合格声明

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声明，并在高风险人工智能系统投放市场或投入服务后 10 年内将其交由成员国主管机关保存。欧盟合格声明应标明所针对的高风险人工智能系统。欧盟合格声明的副本应按要求提交给相关成员国主管机关。

2. 欧盟合格声明应说明有关高风险人工智能系统符合第 2 节规定的要求。欧盟合格声明应包含附件五所列的信息，并应翻译成高风险人工智能系统投放市场或在市场上提供的成员国的成员国主管机关易于理解的语言。

3. 如果高风险人工智能系统受其他欧盟统一立法的约束，而这些立法也要求欧盟合格声明，则应针对适用于高风险人工智能系统的所有欧盟法律起草一份单一的欧盟合格声明。声明应包含所有必要信息，以确定声明所涉及的欧盟统一立法。

4. 通过起草欧盟合格声明，提供者应承担遵守第 2 节所列要求的责任。提供者应及时更新欧盟合格声明。

5. 欧盟委员会有权根据第 97 条通过授权法案，对附件五进行修订，更新该附件中欧盟合格声明的内容，以引入技术发展所需的要素。

第 48 条
CE 标志

1. CE 标志应遵守(EC)第 765/2008 号条例第 30 条规定的一般原则。

2. 对于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，但前提是该标志可通过访问该系统的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。

3. 对于高风险的人工智能系统，CE 标志应明显、清晰和不可擦除地粘贴。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的文件上。

4. 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被通知机构的识别号。被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提供者的授权代表贴上。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。

5. 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 49 条
登记

1. 在将附件三所列的高风险人工智能系统投放市场或投入服务之前，除附件三第 2 项所述的高风险人工智能系统外，提供者或在适用情形下的授权代表应在第 71 条所述的欧盟数据库中登记自己及其系统。

2. 在根据第 6 条第 3 段认定不属于高风险的人工智能系统投放市场或投入使用之前，该提供者或授权代表（如适用）应在第 71 条所述欧盟数据库中登记自己和该系统。

3. 在投入服务或使用附件三所列的高风险人工智能系统之前，除附件三第 2 项所列的高风险人工智能系统外，作为公共机关、欧盟机构、团体、办事处或代理机构的部署者或代表其行事的人员应在第 71 条所述的欧盟数据库中登记、选择系统并登记其使用情况。

4. 对于附件三第 1、6 和 7 项所述执法、移民、庇护和边境管制管理领域的高风险人工智能系统，本条第 1、2 和 3 段所述登记应在第 71 条所述欧盟数据库的一个安全非公开部分进行， 并应在适用的情况下仅包括以下信息：

(a) 附件 八 的 A 部分第 1 至 10 项，但第 6、8 和 9 项除外；
(b) 附件 八 B 部分第 1 至 5 项以及第 8 和 9 项；
(c) 附件 八 的 C 部分第 1 至 3 项；
(d) 附件 九 第 1、2、3 和 5 项。

只有欧盟委员会和第 74 条第 8 段提及的成员国机关可以访问本段第一段所列欧盟数据库中各自的限制访问部分。

5. 附件三第 2 项所指的高风险人工智能系统应在成员国层面登记。

第四章

特定人工智能系统的提供者和部署者的透明度义务

第 50 条
特定人工智能系统的提供者和部署者的透明度义务

1. 提供者应确保，预期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，综合考虑使用的情况和场景，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。

2.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的有效性、互操作性、稳健性和可靠性，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。

3.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、2018/1725 号条例和 2016/680 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，如果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。

4.生成或操纵构成深度伪造的图像、音频或视频内容的人工智能系统的部署者应当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，本段规定的透明度义务限于以不妨碍作品展示或欣赏的适当方式披露存在此类生成或操纵内容。

如果生成或操纵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，相应人工系统的部署者应当披露该文本是人工生成或操纵的。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；或者人工智能生成的内容经过人工审核或编辑控制，而自然人或法人对发布的内容负有编辑责任。

5.第 1 至第 4 段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。

6.第 1 至 4 段不应影响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部署者的其他透明度义务。

7.人工智能办公室应鼓励和促进在欧盟层级起草行为守则，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。欧盟委员会有权根据第 56 条第 6 段规定的程序，通过实施法案批准这些行为守则。如果欧盟委员会认为行为守则不够充分，则有权根据第 98 条第 2 段规定的审查程序，通过一项实施法案，明确规定履行这些义务的共同规则。

第五章

通用人工智能模型

第 1 节
分类规则

第 51 条
将通用人工智能模型归类为具有系统性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而认定其具有高影响力；
(b) 根据欧盟委员会依职权做出的决定，或在科学小组提出有资质的警告后，考虑附件十三设定的标准，认为通用人工智能模型具有与第(a)项相同的能力或影响。

2.根据第 1 段第(a)项，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计大于 10^{25} 时，应推定该模型具有高影响能力。

3. 根据不断发展的技术，如算法的改进或硬件效率的提高，欧盟委员会应当根据第 97 条通过授权法案，修订第 1 段和第 2 段列出的阈值，以及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 52 条
程序

1.如果通用人工智能模型符合第 51 条第 1 段第(a)项所述要求，有关提供者应在满足这些要求或得知将满足这些要求后 2 周内及时通知欧盟委员会。通知应包括必要的信息，以证明相关要求已得到满足。如果欧盟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，欧盟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 51 条第 1 段第(a)项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。

3.如果欧盟委员会得出结论认为，根据第 2 段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，则欧盟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.欧盟委员会可依职权，或在科学小组根据第 90 条第 1 段第(a)项提出有资质的警示后，根

据附件十三规定的标准，指定特定通用人工智能模型具有系统性风险。
欧盟委员会有权根据第 97 条的规定，通过授权法案明确和更新附件十三中的标准。

5.对于根据第 4 段被指定为具有系统性风险的通用人工智能模型，其提供者提出的确有依据的请求，欧盟委员会应予以考虑，并可决定根据附件十三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。如果欧盟委员会在重新评估后决定维持指定为具有系统性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。

6.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 节
通用人工智能模型提供者的义务

第 53 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十一所列的要素，以便应要求向人工智能办公室和成员国主管机关提供；
(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提供者提供信息和文件。在不影响根据欧盟和成员国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) 至少包含附件十二所列内容；
(c) 制定一项尊重欧盟版权法的政策，特别是通过当前技术手段，确定和尊重根据 2019/790 号指令第 4 条第 3 段表达的保留权利；
(d) 根据由人工智能办公室提供的模板，起草并公开有关用于通用人工智能模型训练的内容的足够详细的摘要。

2.第 1 段（a）和（b）项规定的义务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，开源许可允许获取、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性风险的通用人工智能模型。

3.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，应与欧盟委员会和成员国主管机关进行必要的合作。

4.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 56 条所指的行为守则来证明其遵守了第 1 段中的义务。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，或者不遵守欧盟统一标准，应证明有其他适当的合规手段，供欧盟委员会评估。

5.为便于遵守附件十一，特别是第 2 条第(d)和(e)项的规定，欧盟委员会应有权根据第 97 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。

6.根据第 97 条第 2 段的规定，欧盟委员会有权通过授权法案，根据不断发展的技术对附件十一和附件十二进行修订。

7.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 78 条规定的保密义务处理。

第 54 条
通用人工智能模型的授权代表

1.在欧盟市场上投放通用人工智能模型之前，在欧盟之外设立的提供者应通过书面授权，指定一名在欧盟内设立的授权代表，使其能够执行本条例规定的任务。

2. 人工智能模型提供者应使其授权代表能够执行授权书中所规定的任务。

3.授权代表应执行提供者授权书中规定的任务。其应根据要求以欧盟机构的官方语言之一向人工智能办公室提供一份授权书副本。在本条例中，授权书应授权授权代表执行以下任务：
(a) 核查附件十一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 53 条、第 55 条（如果该条适用）规定的所有义务；
(b) 在该通用目的人工智能模型投放市场后的 10 年内，为人工智能办公室和成员国主管机关保存一份附件十一所列举的技术文件副本，以及指定授权代表的提供者的详细联系信息；
(c) 在收到确有依据的要求的情况下，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(b)项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成员国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，包括当该模型集成到在欧盟市场上销售或提供服务的人工智能系统中时；

4.在提供者之外或代替提供者，授权代表应有权在与确保遵守本条例有关的所有问题上，接受人工智能办公室或主管机关的询问。

5.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。

6.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 节
具有系统风险的通用人工智能模型提供者的义务

第 55 条
具有系统风险的通用人工智能模型提供者的义务

1.除第 53 条和第 54 条所列的义务外，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) 评估和减轻欧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，并酌情向成员国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) 确保对具有系统性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第 56 条所指的行为守则来证明遵守了第 1 段的义务。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，供欧盟委员会批准。

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 78 条规定的保密义务处理。

第 4 节
行为守则

第 56 条
行为守则

1.人工智能办公室应综合考虑到国际进路，鼓励和促进在欧盟层级制定行为守则，作为促进本条例正确实施的要件之一。

2.人工智能办公室和委员会应致力于确保行为守则至少应包含第 53 条和第 55 条规定的义务，包括以下要点：
(a) 确保第 53 条第 1 段第(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；
(b) 用于训练的内容摘要的细节的充分性水平：
(c) 确定欧盟层级系统性风险的类型和性质，适当时包括其来源；
(d) 在欧盟层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，这应与风险成比例，考虑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成员国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盟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，并在欧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。

6.人工智能办公室和欧盟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盟人工智能委员会应评估行为守则是否涵盖第 53 条和第 55 条规定的义务，并应定期监督和评估其目标的实现情况。欧盟人工智能委员会应公布其对行为守则充分性的评估结果。

欧盟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 98 条第 2 段规定的审查程序通过。

7.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，这种参与应仅限于第 53 条的义务，除非其明确宣布有兴趣加入完整的守则。

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. 行为守则最迟应在 2025 年 5 月 2 日之前准备完毕。人工智能办公室应采取必要措施，包括根据第 7 段邀请提供者。
如果 2025 年 8 月 2 日行为守则无法准备完毕，或者人工智能办公室认为根据本条第 6 段进行评估后仍不充分，则欧盟委员会可通过实施法案提供共同规则，以履行第 53 条和第 55 条规定的义务，包括本条第 2 段规定的应当包括的要点。这些实施细则应按照第 98 条第 2 段所述的审查程序予以通过。

第六章

支持创新的措施

第 57 条
人工智能监管沙盒

1.成员国应确保其主管机关在国家层级建立至少一个人工智能监管沙盒，该沙盒应在本条例生效 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。欧盟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。

本段第一项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层面的覆盖。

2.还可以在区域或地方层级，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；

3.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成员国主管机关的职责和任务。

4.成员国应确保第 1 段和第 2 段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，成员国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成员国主管机关之间开展适当程度的合作。

5.根据第 1 段建立的人工智能监管沙盒应当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提供服务之前，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。

6.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。

7.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成员国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格性评估程序。

8.在不违反第 78 条的保密规定的前提下，经沙盒提供者或潜在提供者同意，欧盟委员会和欧盟人工智能委员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成员国主管部门明确同意，退出报告可通过本条提及的单一信息平台公开发布。

9.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欧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) 促进基于证据的监管学习；
e) 促进和加快人工智能系统进入欧盟市场，特别是由包括初创企业在内的中小型企业提供的人工智能系统。

10.成员国主管机关应确保，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，则成员国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。

11.人工智能监管沙盒不应影响包括地区或地方层级的主管机构的监督和纠正权力。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，成员国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。成员国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，目的是支持欧盟内的人工智能创新。

12.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。然而，只要潜在提供者遵守具体计划及其参与条款和条件，并且诚实遵循成员国主管机关提供的指导，主管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，则不得在相应立法下处以行政罚款。

13.在设计和实施相关的人工智能监管沙盒时，应促进成员国主管机关之间的跨境合作。

14.成员国主管机关应在欧盟人工智能委员会的框架内协调其活动并开展合作。

15.成员国主管机关应向人工智能办公室和欧盟人工智能委员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。

16.成员国主管机关应向人工智能办公室和欧盟人工智能委员会提交年度报告，从人工智能监管沙盒设立的一年后开始提交，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。欧盟委员会在执行本条例规定的任务时，应酌情考虑年度报告。

17.欧盟委员会应当根据第62条第1段第(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，使得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，欧盟委员会应积极主动地与成员国主管机关进行协调。

第 58 条
人工智能监管沙盒的模式和运作

1.为避免在欧盟内各行其是，欧盟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。
相应实施法案应当根据第 98 条第 2 段提及的审查程序通过。

2.第 1 段提及的实施法案应确保：
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应透明公平，成员国主管机关应在申请后 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，并且能跟上参与的需求；提供者和潜在提供者还可与部署者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成员国主管机关灵活建立和运行其人工智能监管沙盒；
d) 中小型企业和初创企业可免费进入人工智能监管沙盒，但不影响成员国主管机关以公平和成比例的方式对特殊费用收取补贴；
e) 通过人工智能监管沙盒的学习成果，促进提供者和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 95 条提及的行为守则；
f) 人工智能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，如被通知机构和标准化组织、中小型企业、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，参与由成员国或由欧盟数据保护监管机构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。成员国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，特别是中小型企业和初创企业，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、

欧洲数字创新中心和卓越中心方面的帮助。

4.当成员国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，其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，其应与其他成员国主管机关合作，以确保整个欧盟的实践一致。

第 59 条
进一步处理个人数据，以便在人工智能监管沙盒中为公共利益开发特定人工智能系统

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、训练和测试沙盒中的特定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：

(i) 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；

(ii) 高水平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；

(iii) 能源的可持续性；

(iv) 运输系统和流动性、关键基础设施和网络的安全性和韧性；

(v) 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 3 章第 2 节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训练、测试和验证过程及原理，并将预测结果作为附件四的技术文件的一部分；

(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。

2.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欧盟法律，并受制于第 1 段所述的相同累积条件。

3.第 1 段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 60 条
在人工智能监管沙盒之外的真实世界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不应影响第 5 条的禁止规定。
真实世界测试计划的详细内容应在欧盟委员会根据第 98 条第 2 项提及的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真实世界条件下对附件一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提供服务之前的任何时候，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，不得妨碍成员国或欧盟法律可能要求的伦理审查。

4.服务提供者或潜在的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。在成员国法律未规定默许的情况下，真实世界条件下的测试应还需获得授权；
(c) 提供者或潜在提供者已在第 71 条第 4 段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九中规定的信息，但附件三第 1、6 和 7 项所述执法、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 项所述的高风险人工智能系统除外；附件三第 1、6 和 7 项所述的在执法、移民、庇护和边境控制管理领域高风险人工智能系统的提供者或潜在提供者，已根据第 49 条第 4 段第(d)项在欧盟数据库的安全非公共部分注册了真实世界条件下的测试，并使用欧盟范围内唯一的单一识别号码和其中指定的信息；附件三第 2 项所规定的高风险人工智能系统的提供者或潜在提供者已根据第 49 条第 5 段登记了真实世界条件下的测试。
(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定代表；
(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所规定的适当且适用的保障措施下才能传输至第三国；
(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，在任何情况下不应超过 6 个月，但如果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，则可再延长

6 个月；
(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 61 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，其个人数据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，其合法指定的代表可以在没有受到任何损害，也无需提供任何理由的情况下，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。撤销知情同意不会影响已经开展的活动。

6.根据第 75 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高风险人工智能系统进行检查。市场监督管理机关应利用这些权力确保这些真实世界测试的安全发展。

7.在真实世界条件下的测试过程中发现的任何严重事故，应根据本条例第 73 条向成员国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，则应暂停真实世界条件下的测试，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，以便在终止真实世界条件下的测试后立即召回人工智能系统。

8.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世界条件下检测的成员国国家市场监督管理机关。

9.提供者和潜在提供者应根据适用的欧盟和成员国责任法，对其在参与真实世界条件下的测试过程中造成的所有损害承担责任。

第 61 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 60 条的规定在真实世界条件下进行测试，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，自由地作出知情同意：
(a) 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；
(b) 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；
(c) 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世界测试的权利，而不会因此受到任何损害，也无需提供任何理由；
(d) 要求推翻或忽略人工智能系统的预测、建议或决定的方式；
(e) 根据第 60 条第 4 段第(c)项的规定，在真实世界条件下进行测试的欧盟范围内的单一识别号，以及提供者或其法定代表的可向其索取进一步信息的详细联系方式。

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表。

第 62 条
针对提供者和部署者，特别是中小型企业，包括初创企业的措施

1.成员国应采取以下行动：
(a) 在满足资格条件和选择标准的情形中，为在欧盟拥有登记办公室或分支机构的中小型企业（包括初创企业）提供优先进入人工智能监管沙盒的机会。优先准入不应排除本段第一项所述的以外的其他中小型企业（包括初创企业）进入人工智能监管沙盒，只要它们符合资格条件和遴选标准；
(b) 针对中小型企业（包括初创企业），部署者以及适当情况下的地方公共机关需要，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中型企业、部署者、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；
(d) 促进中小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，应考虑到中小型企业（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。

3.人工智能办公室应采取以下行动：
(a) 应欧盟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，为欧盟内所有运营者提供与本条例相关的易于使用的信息；
(c) 组织适当的沟通活动，提高人们对本条例规定的义务的认识；
(d) 在与人工智能系统有关的公共采购程序中评估有关最佳实践并促进其趋同。

第 63 条
特定运营者的克减

1.2003/361/EC 号建议所定义的微型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特定要素。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，制定关于可采取简化方式满足的质量管理系统要素的指南。

2.第 1 段不得解释为免除这些运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、72 和 73 条规定的要求和义务。

第七章

治理

第 1 节
欧盟层面的治理

第 64 条
人工智能办公室

1.欧盟委员会应通过人工智能办公室发展欧盟在人工智能领域的专业知识和能力。
2.成员国应为完成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 65 条
欧盟人工智能委员会的设立和结构

1. 即此成立“欧盟人工智能委员会”（委员会）。

2. 欧盟人工智能委员会应由每个成员国的一名代表组成。欧洲数据保护监督机构作为观察员参加。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成员国和欧盟机关、机构或专家相关，欧盟人工智能委员会可根据具体个案邀请其参加会议。

3. 每位代表由其成员国指定，任期 3 年，可连任一次。

4.成员国应确保其在欧盟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，以便积极促进第 66 条所述欧盟人工智能委员会任务的完成；
(b) 被指定为欧盟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盟人工智能委员会的任务.

5.成员国指定的代表应以三分之二多数通过欧盟人工智能委员会的程序规则。程序规则应特别规定遴选程序、主席任期和具体任务、表决方式以及欧盟人工智能委员会的组织活动安排。

6.欧盟人工智能委员会应设立两个常设工作小组，为市场监督管理机构和被通知机构之间就市场监督管理和通知机关相关问题提供合作和交流的平台。

市场监督管理常设工作小组应作为 2019/1020 号条例第 30 条所指的本条例的行政合作组。

欧盟人工智能委员会可酌情设立其他常设或临时小组以审议具体问题。在适当情况下，可邀请第 67 条提及的咨询论坛代表以观察员身份参加这些小组的具体会议。

7.欧盟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

8.欧盟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盟人工智能委员会任务拟定议程。

第 66 条
欧盟人工智能委员会的任务

欧盟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。尤其在如下方面，欧盟人工智能委员会可以：

(a) 促进负责实施本条例的成员国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 74 条第 11 段所述市场监督管理机关的联合行动；

(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) 协调成员国行政管理实践，包括第 46 条提及的合格性评估程序的克减、第 57、第 59 和第 60 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导意见，制定及适用行为守则；

(ii) 根据第 112 条对本条例进行评估和审查，包括第 73 条提及的严重事件报告和第 71 条提及的欧盟数据库的功能、拟定授权法案或实施法案，以及使本条例与附件一所列法案保持一致的可能性；

(iii) 关于第三章第 2 节所列要求的技术规范或现有标准；

(iv) 第 40 条和第 41 条提及的统一标准或共同规格的使用；

(v) 诸如欧盟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等趋势；

(vii) 人工智能价值链类型的演变趋势，特别是由此产生的对责任的影响；

(vii) 根据第 7 条对附件三进行修正的潜在必要性，以及综合考虑到相关的现有证据和先进技术的水平，根据第 112 条对第 5 条进行可能修订的潜在必要性；

(f) 支持欧盟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) 促进共同标准的制定以及市场运营者和主管机关对本条例规定的相关概念的共识，包括促进基准的制定；

(h) 通过适当方式与欧盟其他机构、机关、 办公室和机构以及相关的欧盟专家组和专家网络开展合作，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) 协助成员国主管机关和欧盟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；

(k) 协助人工智能办公室支持成员国主管机关建立和发展人工智能监管沙盒，并促进监管沙盒之间的合作和信息共享；

(l) 为指导文件的编制做出贡献并提供相关建议；

(m) 就人工智能方面的国际事务向欧盟委员会提供咨询意见。

(n) 就通用人工智能模型的合格警报向欧盟委员会提供意见；

(o) 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 67 条
咨询论坛

1.应当设立一个咨询论坛，向欧盟人工智能委员会和欧盟委员会提供技术知识和咨询意见，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、 中小型企业、民间社会和学术界。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中小型企业和其他企业。

3.欧盟委员会应根据第 2 段规定的标准，从在人工智能领域具有公认专业知识特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、欧盟网络安全局、欧盟标准化委员会、欧盟电子技术标准化委员会和欧盟电信标准协会应为咨询论坛的常任成员。

6.咨询论坛应制定其程序规则。论坛应根据第 2 段规定的标准，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.咨询论坛可应欧盟人工智能委员会或欧盟委员会的要求，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 68 条
独立专家科学小组

1.欧盟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 98 条第 2 段提及的审查程序通过。

2.科学小组应由欧盟委员会根据第 3 段所述任务所需的人工智能领域最新科学或专业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) 具有人工智能领域的专业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。
欧盟委员会应与欧盟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) 支持本条例在通用人工智能模型和系统方面的实施和执行，特别是通过以下方式：
(i) 根据第 90 条的规定，就欧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，包括通过基准测试；
(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) 就各种的通用人工智能模型和系统的分类提供建议；
(v) 协助工具和模板的开发。
(b) 应市场监督管理机关的要求，支持其工作；
(c) 支持第 74 条第 11 段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 81 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.专家应公正客观地履行任务，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。其在执行第 3 段规定的任务时，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冲突说明，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 段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科学小组执行任务的条件、程序和详细安排的规定。

第 69 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.成员国可以被要求为专家的咨询和支持支付费用。费用的结构和水平以及补贴成本的规模和结构应在第 68 条第 1 段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.欧盟委员会应根据需要为成员国及时获得专家支持提供便利，并确保根据第 84 条由欧盟人工智能测试支持部门和根据本条由专家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 节
成员国主管机关

第 70 条
指定成员国主管机关和单一联络点

1.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成员国主管机关。这些成员国主管机关应独立、公正和不带偏见地行使权力，以保障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关来完成。

2.成员国应向欧盟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。

3.成员国应确保向成员国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。特别是成员国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。

4.成员国主管机关应采取适当水平的网络安全措施。

5.成员国主管机关在执行任务时，应遵守第 78 条规定的保密义务。

6.成员国应在本条例生效后的一年内，并在此后每两年向欧盟委员会报告成员国主管机关的财力和人力资源状况，并评估其是否充足。欧盟委员会应将这些信息转交欧盟人工智能委员会讨论并提出可能的建议。

7.欧盟委员会应促进各国主管机关之间的经验交流。

8.成员国主管机关可在适当但情形下考虑欧盟人工智能委员会和欧盟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中小型企业提供指导和建议。当成员国主管机关意图就其他欧盟法所涵盖领域的人工智能系统提供指导和建议时，应在适当但情形下咨询该欧盟法下的成员国主管机关。

9.当欧盟机构、实体、办公室和代理机构属于本条例的适用范围时，欧洲数据保护监督机构应作为主管机关对其进行监督。

第八章

欧盟高风险人工智能系统数据库

第 71 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 段和第 3 段提及的关于第 6 条第 2 段提及的根据第 49 条和第 60 条登记的高风险人工智能系统的信息，以及根据第 6 条第 3 段提及的根据第 49 条登记的不被视为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，欧盟委员会应咨询相关专家；在更新该数据库的功能规格时，欧盟委员会应咨询人工智能委员会。

2.附件八 A 和 B 节所列数据应由提供者录入欧盟数据库，或在适用的情况下由授权代表录入。

3.附件八 C 节所列数据应由公共机关、机构或团体的部署者或其代表根据第 49 条第 3 段和第 4 段输入欧盟数据库。

4.除第 49 条第 4 段和第 60 条第 4 段第(c)项提及的部分外，根据第 49 条登记的欧盟数据库中的信息应以用户友好的方式向公众公开。信息应易于浏览和机器可读。根据第 60 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该信息也向公众开放。

5.欧盟数据库包含个人数据应仅限于根据本条例收集和处理信息所必需。这些信息应包括负责登记系统，以及在适用情况下拥有代表提供者或部署者的法律授权的自然人的姓名和联系方式。

6.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可访问性要求。

第九章

后市场监测、信息共享和市场监督

第 1 节
后市场监测

第 72 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相称的方式，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生命周期内的性能相关数据，并使提供者能够评价人工智能系统是否持续符合第 3 章第 2 节规定的要求。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交互。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 2026 年 2 月 2 日以前通过一项实施法案，详细规定后市场监测计划的模板条款和计划应包括的内容清单。该实施法案应按照第 98 条第 2 段所述审查程序通过。

4.对于附件一 A 节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 段所述模板，将第 1、第 2 和第 3 段所述必要内容纳入附件一 A 节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。

本段第一项也适用于附件三第 5 项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服务。

第 2 节
共享严重事故的信息

第 73 条
严重事故的报告

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。

2.第 1 段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，或者在适用情况下的部署者，意识到严重事故之后 15 天。
本段第 1 分段所述的报告期限应考虑到严重事故的严重性。

3.尽管有第 2 段的规定，如果发生第 3 条第 49 段第(b)项定义的大范围违规或严重事故，应立即提交本条第 1 段所述的报告，且不得迟于提供者，或者在适用情况下的部署者，意识到该事件后的两天。

4.尽管有第 2 段的规定，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，或者在适用情况下的部署者，意识到严重事故之日起 10 天。

5.为确保及时报告，提供者，或者在适用情况下的部署者，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。

6.在根据第 1 段报告严重事故后，提供者应立即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。
在第一分段所指的调查期间，提供者应与主管机关合作，并在相关情况下与有关被通知机构合作。在向主管机关通报此类行动之前，不得进行任何涉及改变相关人工智能系统的调查，从而可能影响对事件原因的任何后续评估。

7.在收到与第 3 条第 49 段第(c)项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 77 条第 1 段所述的成员国公共机关或机构。欧盟委员会应制定专门指南，以促进遵守本条第 1 段规定的义务。该指南最迟应在 2025 年 8 月 2 日前发布，并应定期评估。

8.市场监督管理机关应在收到第 1 段所述通知之日起 7 天内采取 2019/1020 号条例第 19 条规定的适当措施，并应遵循 2019/1020 号条例规定的通知程序。

9.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服务的提供者受制于规定了与本条例同等报告义务的欧盟立法工具，则严重事故的通报应仅限于第 3 条第 49 段第(c)项所述的情况。

10.对于属于 2017/745 号条例和 2017/746 号条例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 49 段第(c)项中提及的事故，并应向事故发生地成员国为此目的选择的成员国主管机关通报。

11.无论欧盟委员会是否已就此采取行动，成员国主管机关应根据 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故。

第 3 节
执法

第 74 条
欧盟市场中的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。为了有效执行本条例：
(a) 凡提及 2019/1020 号条例的经济运营者，均应理解为包括本条例第 2 条第 1 段确定的所有运营者；
(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 段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禁止性实践的情况以及所采取的措施。

3.对于与附件一 A 节所列欧盟统一立法所涵盖产品有关的高风险人工智能系统，出于本条例的目的，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，成员国可以通过克减第一分段，指定另一个相关机构作为市场监督管理机关，但须确保与负责执行附件一所列欧盟统一立法的相关部门市场监督管理机关进行协调。

4. 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，则本条例第 79 至 83 条所述程序不适用于附件一 A 节所列欧盟统一立法所涵盖产品有关的人工智能系统。在这类情形中，应适用相关部门的程序。

5. 在不影响 2019/1020 号条例第 14 条规定的市场监督管理机关权力的情况下，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 段第(d)项和(j)项所述的权力。
6.对于由受欧盟金融服务立法监管的金融机构投放市场、投入服务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、投入服务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。

7.在有正当理由的情况下，并在确保协调的前提下，成员国可通过对第 6 段的克减，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(EU)2013/36 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 号法规建立的单一监管机制 (SSM)，则应立即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。

8.对于附件三第 1 项所列的高风险人工智能系统，只要该系统用于执法目的、边境管理、司法和民主、以及附件三第 6、7 和 8 项所列目的，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 41 至 44 条规定的相同条件指定的任何其他机构，作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。

9.如果欧盟机构、主体、办公室或代理机构属于本条例的适用范围，则欧洲数据保护监督机

构应作为其市场监督管理机关行事，但与以司法权限行事的欧盟法院有关的情况除外。

10. 对于其他相关国家机关或机构负责监督附件一所列欧盟统一立法，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的机关或机构，成员国应促进根据本条例指定的市场监督管理机关与它们的协调。

11.市场监督管理机关和欧盟委员会应能够提议开展联合行动，包括由市场监督管理机关开展调查，或由市场监督管理机关与欧盟委员会联合开展的调查，其目的是促进合规、查明不合规情况、提高对本条例的认识，并针对被发现在两个或更多成员国构成严重风险的特定类别高风险人工智能系统，根据 2019/1020 号文件第 9 条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。

12.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训练、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或其他相关技术手段和工具实现远程访问。

13.市场监督管理机关应在合理请求的情况下，并仅在满足以下两个条件的情况下，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章第 2 节的要求，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/审计程序和核查程序已经用尽，或者已被证明不充分。

14.市场监督管理机关获得的任何信息和文件，均应按照第 78 条规定的保密义务处理。

第 75 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本节和 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，并相应地通知委员会和其他市场监督管理机关。

3.当一个成员国市场监督管理机关已做出一切适当努力来获得这些信息，但仍无法获得与人工智能模型有关的特定信息，从而无法完成对高风险人工智能系统的调查时，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的访问权。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。市场监督管理机关应根据第 78 条的规定对所获得的信息保密。1020/2019 号条例第 6 章规定的程序应比照适用。

第 76 条
市场监督管理机关对真实世界条件下测试的监督

1.市场监督管理机关应有能力和权力确保，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 58 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 60 条规定的合规情况，作为其人工智能监管沙盒的监管角色的一部分。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 60 条第 4 段第(f)和(g)项规定的条件。

3.如果市场监督管理机关已从潜在提供者、提供者或任何第三方知晓发生了严重事故，或有其他理由认为第 60 条和第 61 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) 暂停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部署者或潜在部署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作出本条第 3 段所述的决定，或已发出第 60 条第 4 段第(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如何对该决定或反对意见提出质疑。

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 段所述的决定，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 77 条
保护基本权利的机关的权力

1.监督或执行保护欧盟法律规定的基本权利（包括不受歧视的权利在内的与附件三所规定的高风险人工智能系统使用相关的基本权利）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。

2.在 2024 年 11 月 2 日前，各成员国应确定第 1 段提及的公共机关或机构，并公布其名单。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。

3.如果第 1 段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 1 段提及的公共机关或机构可向市场监督管理机关提出确有依据的请求，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。

4.第 1 段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 78 条规定的保密义务处理。

第 78 条
保密性

1.欧盟委员会、市场监督管理机关和被通知机构，以及参与实施本条例的任何其他自然人或法人，应根据欧盟或成员国法律，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，但欧盟议会和理事会 2016/943 号指令第 5 条所述的情况除外。
(b) 本条例的有效实施，特别是为了检查、调查或审计的目的；
(c) 公共和国家安全利益；
(d) 刑事或行政诉讼的开展；
(e) 根据欧盟或成员国法律归类为保密的信息。

2.根据第 1 段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。其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，并应根据适用的欧盟或成员国法律，在不再需要用于所请求的目的时，立即删除所收集的数据。

3.在不影响第 1 段和第 2 段的情况下，当执法、边境管制、移民或庇护机关使用附件三第 1、6 和 7 项所述高风险人工智能系统时，对于在成员国主管机关之间以及成员国主管机关与欧盟委员会之间基于保密基础的交流信息，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成员国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 项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 74 条第 8 段和第 9 段所指的市场监督管理机关在适用的情况下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。

4.第 1 段、第 2 段和第 3 段不影响欧盟委员会、成员国及其有关机关以及被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。

5.必要时，欧盟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 79 条
处理在成员国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 项所定义的“具有风险的产品”。

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 段所述的风险，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。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 77 条第 1 段所述的相关国家公共机关或机构，并与之充分合作。相关运营者应与市场监督管理机关和第 77 条第 1 段所述的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或与第 77 条第 1 段所述国家公共机构合作的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，要求相关运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召回。

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 2 段所述措施。

3.如果市场监督管理机关认为不合规的情况不限于本国境内，则应将评估结果和要求运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。

4.运营者应确保对其在欧盟市场上投放的所有相关人工智能系统采取了一切适当的纠正措施。

5.如果人工智能系统的运营者在第 2 段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服务，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。该机关应立即将这些措施通知欧盟委员会和其他成员国。

6.第 5 段所述通知应包括所有现有的细节，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运营者提出的论据。市场监督管理机关应特别说明，不合规的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；
(b) 高风险人工智能系统未能达到第三章第 2 节规定的要求；
(c) 第 40 条和第 41 条所述的推定合规的统一标准或共同规格中的缺陷；
(d) 不遵守第 50 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立即向欧盟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合规有关的任何补充信息，并在不同意被通报国家措施的情况下，应通报其反对意见。

8.如果在收到第 5 段所述通知后的三个月内，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。这不影响相关运营者根据 2019/1020 号条例第 18 条享有的程序权利。在不遵守本条例第 5 条所述的禁止的人工智能实践的情况下，本段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，如及时将产品或人工智能系统撤出其市场。

第 80 条
处理提供者在适用附件三时被归类为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的理由认为，提供者在适用第 6 条第 3 段时被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第 6 条第 3 段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，其应立即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，并在其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欧盟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未能在第 2 段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 99 条对提供者处以罚款。

5.提供者应确保对其在欧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 段所述期限内未能采取适当的纠正措施，则适用第 79 条第 5 至第 9 段的规定。

7.如果在根据第 1 段进行评估的过程中，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，以规避适用第三章第 2 节的要求，则应根据第 99 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 71 条所述的欧盟数据库中存储的信息。

第 81 条
欧盟保障程序

1.在收到第 79 条第 5 段所述的通知后的 3 个月内，或在不遵守第 5 条所述的禁止人工智能实践的情况下的 30 日内，如果一个成员国的市场监督管理机关对另一个成员国的市场监督管理机关采取的措施提出异议，或者如果欧盟委员会认为该措施违反欧盟法律，欧盟委员会应立即与相关成员国的市场监督管理机关和运营者进行协商，并对该成员国措施进行评估。根据评估结果，欧盟委员会应在第 65 条第 5 段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 日内，决定该成员国措施是否合理，并将该决定通知相关成员国的市场监督管理机关。欧盟委员会还应将此决定通知所有其他市场监督管理机关。

2.如果欧盟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，如要求其及时从其市场上撤回人工智能系统的行为，并应将有关情况通知欧盟委员会。如果欧盟委员会认为成员国措施不合理，有关成员国应撤销该措施并向欧盟委员会通报。

3.如果成员国的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 条中所述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 82 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根据第 79 条进行评估，并向第 77 条第 1 段提及的相关国家公共机关咨询后，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，则应要求相关运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服务时，在其可加以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者应确保在第 1 段所述成员国市场监督管理机关规定的时限内，对其在欧盟市场上提供的所有相关人工智能系统采取纠正行动。

3.成员国应立即将第 1 段规定的调查结果通知欧盟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.欧盟委员会应及时与有关成员国和相关运营者进行磋商，并对各国采取的措施进行评估。根据评估结果，欧盟委员会应决定该措施是否合理，并在必要时提出其他适当的措施。

5.欧盟委员会应立即将其决定通知有关成员国和相关运营者。欧盟委员会还应将其决定通知所有其他成员国。

第 83 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规定的期限内停止有关违规行为：

(a) 违反第 48 条规定加贴 CE 标志的行为；
(b) 未加贴 CE 标志；
(c) 未准备第 47 条规定的欧盟合格性声明；
(d) 未正确准备第 47 条规定的欧盟合格性声明；
(e) 未按照第 71 条要求在欧盟数据库中登记；
(f) 在适用的情况下，未指定授权代表。
(g) 不具备技术文件。

2.如果第 1 段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对应的措施，限制或禁止高风险人工智能系统在市场上提供，或确保立即从市场上召回或撤回该系统。

第 84 条
欧盟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，以执行 2019/1020 号条例第 21 条第 6 段所列的任务。

2.在不影响第 1 段所述任务的前提下，欧盟人工智能检测支持结构还应根据欧盟人工智能委员会、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 4 节
救济措施

第 85 条
向市场监督管理机关投诉的权利

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 号条例，此类投诉应综合考虑开展市场监督活动的目的，并按照市场监督管理机关制定的专门程序进行处理。

第 86 条
个体决策的解释权

1.任何受到部署者根据附件三所列高风险人工智能系统（第 2 项所列系统除外）的输出结果所做的决定影响的人，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 段不适用于根据欧盟法律或国家法律对第 1 段规定的义务有例外或限制的人工智能系统的使用。
3.本条仅在第 1 段所述的权利尚未在欧盟法律中做出规定的程度上适用。

第 87 条
违规行为的举报和对举报人的保护

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的举报人的保护。

第 5 节
对通用人工智能模型提供者的监督、调查、执法和监测

第 88 条
通用人工智能模型提供者义务的执行

1.欧盟委员会拥有监督和执行第五章的专属权力，同时考虑第 94 条规定的程序保障。欧盟委员会应委托欧洲人工智能办公室执行这些任务，但不得损害欧盟委员会的组织权力以及成员国和欧盟之间根据条约进行的权限划分。

2.在不影响第 75 条第 3 段的情况下，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且成比例的。

第 89 条
监测行动

1.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投诉。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系点；
(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，包括在适当情况下主动收集的信息。

第 90 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出现以下情况时，可向人工智能办公室发出有资质的警报：
(a) 通用人工智能模型在欧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第 51 条所指的要求。

2.在接到这种有资质的警报后，欧盟委员会通过人工智能办公室，并在通知欧盟人工智能委员会后，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 91-94 条规定的任何措施通知欧盟人工智能委员会。

3.有资质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，包括在适当情况下主动收集的信息。

第 91 条
要求提供文件和信息的权力

1.欧盟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第 53 条和第 55 条起草的文件，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，欧盟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，条件是根据第 68 条第 2 段的规定，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.信息请求应说明请求的法律依据和目的，具体说明需要哪些信息，并规定提供信息的期限，并注明第 101 条规定的对提供不正确、不完整或误导性信息的罚款。

5. 有关通用人工智能模型的提供者或其代表应提供所要求的信息。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 92 条
进行评估的权力

1.人工智能办公室在咨询欧盟人工智能委员会后，可对有关的通用人工智能模型进行评估：
(a) 在根据第 91 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) 在欧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第 90 条第 1 段第(a)项提出有资质的警告之后。

2.欧盟委员会可决定任命独立专家代表其进行评估，包括根据第 68 条从科学小组中任命独立专家。为这一任务而任命的所有独立专家均应符合第 68 条第 2 段规定的标准。

3.为第 1 段的目的，欧盟委员会可要求通过应用程序接口或其他适当的技术手段和工具，包括通过源代码，访问通用人工智能模型。

4.访问申请应说明申请的法律依据、目的和理由，并规定提供访问的期限，以及第 101 条规定的对不提供访问的罚款。

5. 有关通用人工智能模型的提供者或其代表应提供所要求的信息。如果是法人、公司或企业，或者如果不具备法人资格，则应由法律或其章程授权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 98 条第 2 段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结构性的对话，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 93 条
要求采取措施的权力

1.在必要和适当的情况下，欧盟委员会可要求提供者：
(a) 采取适当措施以遵守第 53 条和第 54 条所规定的义务；

(b) 要求提供者实施缓解措施，如果根据第 92 条进行的评估引起了对欧盟层面系统性风险的严重且现实的担忧；
(c) 限制在市场上销售，撤回或召回该模型。

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结构性的对话。

3.如果在第 2 段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，以应对欧盟层面的系统性风险，则欧盟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 94 条
通用人工智能模型经济运营者的程序性权利

对于通用人工智能模型的提供者，2019/1020 号条例第 18 条可以比照适用，但不影响本条例中规定的更具体的程序性权利。

第十章

行为守则和指南

第 95 条
自愿适用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章第 2 节中的部分或全部要求，同时考虑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，促进制定有关对所有人工智能系统自愿适用(包括部署者自愿适用)的具体要求的行为守则，包括但不限于：
(a) 欧洲可信人工智能伦理准则中提供的可适用要件；
(b) 评估并最大限度地减少人工智能系统对环境可持续发展的影响，包括节能编程和高效设计、训练和使用人工智能；
(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体提供者或部署者，或代表它们的组织，或由两者共同拟订，拟定者可由任何感兴趣的利益相关者及其代表组织的参与，包括公民社会组织和学术界。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中小型企业的具体利益和需要。

第 96 条
欧盟委员会关于实施本条例的指南

1.欧盟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 25 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 50 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一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) 第 3 条第 1 段中关于人工智能系统的定义的适用。

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中小型企业、地方公共机关以及最有可能受本条例影响的部门的需求。

本段第一项提到的指南应适当考虑人工智能方面的普遍被认可的技术发展水平，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.欧盟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，应当更新已经通过的指南。

第十一章

授权和委员会程序

第 97 条
行使授权

1.根据本条规定的条件，欧盟委员会有权通过授权法案。

2.应当授权欧盟委员会第 6 条第 6 段和第 7 段、第 7 条第 1 段和第 3 段、第 11 条第 3 段、第 43 条第 5 段和第 6 段、第 47 条第 5 段、第 51 条第 3 段、第 52 条第 4 段和第 53 条第 5 段和第 6 段提及的通过授权法案的权力，自 2024 年 8 月 1 日起为期五年。欧盟委员会应在五年期限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其延长，否则授权期限应默许延长至相同期限。

3.第 6 条第 6 段和第 7 段、第 7 条第 1 段和第 3 段、第 11 条第 3 段、第 43 条第 5 段和第 6

段、第 47 条第 5 段和第 51 条第 3 段、第 52 条第 4 段和第 53 条第 5 段和第 6 段提及的授权可随时由欧洲议会或欧盟理事会撤销。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》上公布的次日或其具体规定的日期生效。该决定不影响任何已生效的授权法案的有效性。

4.在通过授权法案之前，欧盟委员会应根据《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，咨询各成员国指定的专家。

5.欧盟委员会一旦通过授权法案，应同时通知欧洲议会和欧盟理事会。

6.根据第 6 条第 6 段和第 7 段、第 7 条第 1 段和第 3 段、第 11 条第 3 段、第 43 条第 5 段和第 6 段、第 47 条第 5 段和第 51 条第 3 段、第 52 条第 4 段和第 53 条第 5 段和第 6 段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 98 条
法案咨询委员会程序

1.欧盟委员会应当由一个法案咨询委员会协助工作。该委员会应为 182/2011 号条例所指的法案咨询委员会。
2.在提及本段时，应适用 182/2011 号条例第 5 条。

第十二章

罚则

第 99 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运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，并应考虑欧盟委员会根据第 96 条发布的指南，采取一切必要的措施确保这些规则和措施得到适当和有效的执行。规定的处罚应当有效、适度并具有威慑性。处罚应考虑包括初创企业在内的中小型企业的利益及其经济可行性。

2.成员国应立即将各自的规则和措施通知欧盟委员会，最迟在这些规则和措施生效之日通知欧盟委员会，并应立即将随后对其产生影响的任何修正通知欧盟委员会。

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 35000000 欧元的行政罚款，如果违规者是企业，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被通知机构有关的规定，将被处以最高 15000000 欧元的行政罚款，如果违规者是企业，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 16 条规定的提供者义务；
(b) 第 22 条规定的授权代表的义务；
(c) 第 23 条规定的进口商的义务；
(d) 第 24 条规定的分销商的义务；
(e) 第 26 条规定的部署者的义务；
(f) 根据第 31 条、第 33 条第 1 段、第 3 段、第 4 段、第 34 条的被通知机构的要求和义务；
(g) 第 50 条规定的提供者和使用者的透明度义务。

5.在回应要求时向通知机关和成员国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；如果违法者是企业，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。

6.对于包括初创企业在内的中小型企业，本条所指的每项罚款应达到第 3、4、5 段所指的百分比或金额，以其中较低者为准。

7.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；
(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运营者的同一违法行为处以行政罚款；
(c) 同一运营者是否因违反其他欧盟或成员国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作为或不作为造成的；
(d) 侵权运营者的规模、年营业额和市场份额；
(e) 适用于案件情节的任何其他加重或减轻处罚的因素，如直接或间接地从侵权行为中获得的经济利益或从中避免的损失。
(f) 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成员国主管机关合作的程度；
(g) 综合考虑运营者采取的技术和组织措施后的运营者责任的程度；
(h) 成员国主管机关知晓侵权行为的方式，特别是运营者是否通知了侵权行为，通知的程度如何；
(i) 侵权行为的故意或过失性质；
(j) 运营者为减轻受影响者所遭受的损害而采取的任何行动。

8.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。

9.根据成员国的法律制度，行政罚款规则的适用方式可以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。

10.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。

11.成员国应每年向欧盟委员会报告其在该年度内根据本条规定所作出的行政罚款，以及任

何相关的诉讼或司法程序。

第 100 条
对欧盟机关、机构、办公室和专门机构的行政罚款

1.欧洲数据保护监督机构可对本条例范围内的欧盟机关、机构、办公室和专门机构处以行政罚款。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，综合考虑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，以及任何相关的在先侵权行为；
(b) 欧盟机关、机构、办公室或专门机构的责任程度，综合考虑其实施的技术和组织措施；
(c) 欧盟机关、机构、办公室或专门机构为减轻受影响者所遭受的损害而采取的任何行动；
(d) 与欧洲数据保护监督机构合作的程度，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机构以前就同一主题事项对有关欧盟机构或机关或团体下令采取的任何措施；
(e) 欧盟机关、机构、办公室或专门机构之前的任何类似违规行为；
(f) 欧洲数据保护监督机构知晓侵权行为的方式，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；
(g) 机构的年度预算。

2.不遵守第 5 条所述的禁止性人工智能实践的规定，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，对任何不遵守本条例规定的要求或义务的人工智能系统处以最高 750000 欧元的行政罚款。

4. 对于欧洲数据保护监督机构诉讼程序管辖的欧盟机关、机构、办公室或专门机构，在根据本条做出决定之前，欧洲数据保护监督机构应给予它们就可能的侵权事项陈述意见的机会。欧洲数据保护监督机构应仅根据有关各方能够发表意见的内容和情况做出决定。如果有投诉人，则投诉人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机构的档案。

6.根据本条规定征收的罚款应纳入欧盟总预算。罚款不得影响被罚款的欧盟机关、机构、办公室或专门机构的有效运作。

7.欧洲数据保护监督员应每年向欧盟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 101 条
对通用人工智能模型提供者的罚款

1. 当欧盟委员会发现提供者故意或疏忽地从事下列行为时，欧盟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 15000000 欧元的罚款，以金额

较高者为准：
(a) 违反本条例的有关规定；
(b) 未遵守第 91 条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；
(c) 未遵守第 93 条要求采取的措施；
(d) 未向欧盟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访问权，以便其根据第 92 条进行评估。

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。欧盟委员会还应考虑根据第 93 条第 3 段做出的承诺或根据第 56 条在相关行为守则中做出的承诺。

2.在根据本条第 1 段通过决定之前，欧盟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性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。

3.根据本条规定处以的罚款应适度、有效并具备威慑性。

4.有关罚款的信息也应酌情通报欧盟人工智能委员会。

5. 对于审查欧盟委员会确定罚款数额的决定，欧盟法院拥有不受限制的管辖权。法院可取消、减少或增加罚款。

6.欧盟委员会应就根据第 1 段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 98 条第 2 段提及的审查程序通过。

第十三章

最终条款

第 102 条
修订(EC)300/2008 号条例

在(EC)300/2008 号条例第 4 条第 3 段中，增加以下分段：
“在采取和欧洲议会和欧盟理事会 2024/...号条例*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章第 3 节规定的要求。”

第 103 条

* 欧洲议会和欧洲理事会.....第 2024/.....号条例，规定了人工智能的统一规则，并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

修订(EU) No 167/2013 条例

在(EU) No 167/2013 条例第 17 条第 5 段中，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(EU) 2024/1689 条例*，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章第 2 节规定的要求。

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 104 条
修订(EU) No 168/2013 条例

在(EU) No 168/2013 条例第 22 条第 5 段中，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(EU) No 168/2013 条例*，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章第 2 节规定的要求。

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 105 条
修订 2014/90/EU 指令

在 2014/90/EU 指令第 8 条中，增加以下段：

“5.对于属于欧洲议会和欧盟理事会条例(EU) 2024/1689 条例*所指安全组件的人工智能系统，欧盟委员会在根据第 1 段开展活动以及根据第 2 段和第 3 段通过。欧盟委员会在根据第 1 段开展活动和根据第 2 段和第 3 段通过技术规范和测试标准时，应考虑该条例第三章第 2 节中的要求。”

* 欧洲议会和欧洲理事会.....第 2024/.....号条例，规定了人工智能的统一规则，并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 106 条
修订(EU) 2016/797 指令

在(EU) 2016/797 指令第 5 条中，增加以下段：

“12.在根据第 1 段通过涉及欧洲议会和欧盟理事会(EU) 2024/1689 条例*所指安全组件的人工智能系统的授权法案和根据第 11 段通过实施法案时，应考虑到该条例第三章第 2 节规定的要求。”

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 107 条
修订(EU) 2018/858 条例

在(EU) 2018/858 条例第 5 条中，增加以下段：

“4.在根据第 3 段通过关于欧洲议会和欧盟理事会(EU) 2024/1689 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章第 2 节规定的要求。”

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 108 条
修订 2018/1139 号条例

2018/1139 号条例修订如下：

(1)在第 17 条中，增加以下段：

“3.在不影响第 2 段的情况下，在根据第 1 段通过有关属于欧洲议会和欧盟理事会 2024/..号条例*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章第 2 节规定的要求。”

(2)在第 19 条中，增加以下段：

“4.在根据第 1 段和第 2 段通过有关属于欧洲议会和欧盟理事会(EU) 2024/1689 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章第 2 节规定的要求。”

(3)在第 43 条中，增加以下段：

“4.在根据第 1 段通过有关属于欧洲议会和欧盟理事会(EU) 2024/1689 条例*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章第 2 节规定的要求。”

(4)在第 47 条中，增加以下段：

“3.在根据第 1 段和第 2 段通过有关属于欧洲议会和欧盟理事会(EU) 2024/1689 条例*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章第 2 节中规定的要求。”

(5)在第 57 条中，增加以下分段：

“在通过有关属于欧洲议会和欧盟理事会 (EU) 2024/1689 条例*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章第 2 节规定的要求。”

(6)在第 58 条中，增加以下段：

“3.在根据第 1 段和第 2 段通过有关属于欧洲议会和欧盟理事会(EU) 2024/1689 条例*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章第 2 节规定的要求。”

---

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。
* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。
* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。
* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。
* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。
* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 109 条
修订(EU) 2019/2144 条例

在(EU) 2019/2144 条例第 11 条中，增加以下段：

"3.在根据第 2 段通过有关属于欧洲议会和欧盟理事会 (EU) 2024/1689 条例*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章第 2 节规定的要求。

* 欧洲议会和欧洲理事会.....第 2024/.....号条例, 规定了人工智能的统一规则, 并修订了第 300/2008 号条例、第 167/2013 号条例、第 168/2013 号条例、第 2018/858 号条例、第 2018/1139 号条例和第 2019/2144 号条例以及 2014/90 号指令、2016/797 号指令以及 2020/1828 号指令(人工智能法案》(OJL,.....,ELI:.....)。

第 110 条
修订(EU) 2020/1828 指令

在欧洲议会和欧盟理事会指令 (EU) 2020/1828 的附件中，增加以下内容：
“(68) 欧洲议会和欧盟理事会第(EU) 2024/1689 条例制定有关人工智能的统一规则，并修订了(EC) No 300/2008 条例、(EU) No 167/2013 条例、(EU) No 168/2013 条例、(EU) 2018/858 条例、(EU) 2018/1139 条例 、 (EU) 2019/2144 条例和 2014/90/EU 指令、 (EU) 2016/797 指令 、 (EU) 2020/1828 （人工智能法案）(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)”。

第 111 条
已经投放市场或投入服务的通用人工智能系统

1.在不影响第 113 条第 3 段(a)项所述的第 5 条适用的情况下，属于附件十所列法案所建立的大型信息技术系统组成部分的、在 2027 年 8 月 2 日前已投放市场或投入服务的人工智能系统，应当在 2030 年 12 月 31 日前符合本条例的规定。
在对附件十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 113 条第 3 段第(a)项所述的第 5 条的适用的情况下，本条例应适用于高风险人工智能系统的运营者，但在 2026 年 8 月 2 日之前已投放市场或投入使用的本条第 1 段所述的系统除外；但除外的情形仅限于自该日期起这些系统的设计发生重大变化的情况。无论如何，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 2030 年 8 月 2 日前采取必要步骤遵守本条例的要求。

3.在 2025 年 8 月 2 日之前已经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 2027 年 8 月 2 日之前遵守本条例规定的义务。

第 112 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和第 5 条禁止的人工智能实践的清单是否需要修订，直至第 97 条设立的授权期结束。欧盟委员会应将评估结果提交欧洲议会和欧盟理事会。

2.在 2028 年 8 月 2 日前以及此后每四年内，欧盟委员会应评估并向欧洲议会和理事会报告：
(a) 是否有必要修订扩大附件三中现有领域或增加新领域；
(b) 对第 50 条中需要额外透明度措施的人工智能系统列表的修正案；
(c)加强监督和治理体系的有效性的修正案；

3. 在 2028 年 8 月 2 日前以及此后每四年内，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欧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。报告应予公布。

4.第 2 段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其任务而拥有的财力、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 99 条第 1 段所指的行政罚款；
(c) 为支持本条例而采用的统一标准和共同规格；
(d) 条例生效后进入市场的企业数量，其中有多少是中小型企业。

5. 在 2028 年 8 月 2 日前以及此后每四年内，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。

6. 在 2028 年 8 月 2 日前以及此后每四年内，欧盟委员会应提交一份关于通用人工智能模型节能开发的标准化交付成果的进展情况审查报告，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欧盟理事会，并应予以公布。

7. 在 2028 年 8 月 2 日前以及此后每三年内，欧盟委员会应评估自愿行为守则的影响和有效性，以促进第三章第 2 节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。

8.为第 1 段至第 7 段之目的，欧盟人工智能委员会、成员国和成员国主管机关应按欧盟委员会的要求向其提供信息，不得无故拖延。

9.在进行第 1 段至第 7 段所述的评估和审查时，欧盟委员会应考虑欧盟人工智能委员会、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。

10.如有必要，欧盟委员会应提交适当的建议来修订本条例，特别是要考虑技术的发展、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。

11.为指导本条第 1 段至第 7 段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：
(a) 附件三所列清单，包括扩展该附件中现有的领域或增加新的领域；
(b) 第 5 条规定的禁止的人工智能实践的清单；以及
(c) 根据第 50 条需要采取额外透明度措施的人工智能系统清单。

12.根据本条第 10 段对本条例的任何修正，或今后涉及附件一 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，以及现有的治理、合格性评估和执行机制以及在这些部门建立的主管机构。

13. 在 2031 年 8 月 2 日前，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欧盟机构来解决任何已经识别的缺陷。

第 113 条
生效和适用

本条例自其在《欧盟官方公报》上公布后第 20 天起生效。

本条例自 2026 年 8 月 2 日起适用，但：
(a) 第一章和第二章自 2025 年 2 月 2 日起起适用；
(b) 除 101 条外，第三章第 4 节、第五章、第七章和第十二章和第 78 条应在 2025 年 8 月 2 日起适用；
(c) 第 6 条第 1 段和本条例中的相应义务自 2027 年 8 月 2 日起适用。

本条例以其整体具备约束力，并直接适用于所有成员国。
在 2024 年 6 月 13 日、布鲁塞尔定稿

欧洲议会　　欧盟理事会
主席　　主席
萝伯塔·梅索拉　　夏尔·米歇尔

附件一

欧盟统一立法清单

A 节. 基于新立法框架的欧盟统一立法清单

1.欧洲议会和欧盟理事会 2006 年 5 月 17 日发布的关于机械，并修订 95/16/EC 号指令的 2006/42/EC 号指令（官方公报，157，2006 年 6 月 9 日，第 24 页）；

2.欧洲议会和欧盟理事会 2009 年 6 月 18 日发布的关于玩具安全的 2009/48/EC 号指令，（官方公报，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 日发布的关于娱乐船只和个人水上设备，并废止指令 94/25/EC 号指令的 2013/53/EU 号指令（官方公报，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 日发布关于统一成员国有关电梯及其安全组件的法律的 2014/33/EU 号指令（官方公报，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 日发布的关于统一成员国有关用于潜在爆炸性环境中的设备和保护系统的法律的 2014/34/EU 号指令（官方公报，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法律，并废止 1999/5/EC 号指令的 2014/53/EU 号指令（官方公报，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 日关于统一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，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，并废止 2000/9/EC 号指令的 2016/424 号条例（官方公报，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，并废止理事会 89/686/EEC 号指令的 2016/425 号条例（官方公报，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，并废止 2009/142/EC 号指令的 2016/426 号条例（官方公报，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，并修订 2001/83/EC 号指令、178/2002 号条例和 1223/2009 号条例，以及废止欧盟理事会 90/385/EEC 号和 93/42/EEC 号

指令的 2017/745 号条例（官方公报，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，并废止 98/79/EC 号指令和 2010/227/EU 号欧盟委员会决定的 2017/746 号条例（官方公报，117，2017 年 5 月 5 日，第 176 页）。

B 节. 欧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，并废止 2320/2002 号条例的 300/2008 号条例（官方公报，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，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，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 日关于海事设备，并废止欧盟理事会 96/98/EC 号指令的 2014/90/EU 号指令（官方公报，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，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，并修订 715/2007 号和 595/2009 号条例，并废止 2007/46/EC 号指令的 2018/858 号条例（官方公报，151，2018 年 6 月 14 日，第 1 页）；

19.欧洲议会和欧盟理事会 2019 年 11 月 27 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在一般性安全和保护车内人员及易受伤害的道路使用者方面的基于类型的批准要求，并修订欧洲议会和欧盟理事会 2018/858 号条例，并废止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、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 号条例的 2019/2144 号条例(官方公报，325，2019 年 12 月 16 日，第 1 页);

20.欧洲议会和欧盟理事会 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，并修订 2111/2005 号、1008/2008 号、996/2010 号、376/2014 号条例以及欧洲议会和欧盟理事会 2014/30/EU 和 2014/53/EU 号指令，并废止欧洲议会和欧盟理事会条例 552/2004 号和 216/2008 号以及欧盟理事会 3922/91 号条例的 2018/1139 号条例（官方公报，212，2018 年 8 月 22 日，第 1 页），就其第 2 条第 1 段第 α 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

第 5 条第 1 分段第 1 项第(h)(iii)点所述刑事犯罪清单

第 5 条第 1 段第 1 项第(h)(iii)点所述刑事犯罪：

- 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，
- 蓄意破坏，
- 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 段提及的高风险人工智能系统

第 6 条第 2 段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，只要相关欧盟或成员国法律允许使用：

(a) 远程生物识别系统。

这不包括其唯一目的是确认特定自然人就是其声称的那个人的用于生物验证的人工智能系统；

(b) 根据敏感或受保护的属性或特征、基于这些属性或特征的推断，意图用于生物分类的人工智能系统。

(c) 拟用于情感识别的人工智能系统。

2.关键基础设施：拟用作关键数字基础设施、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。

(c) 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适当教育水平的人工智能系统；

(d) 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、工人管理和获得自我雇佣的机会：

(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) 旨在用于做出影响工作相关的关系，晋升和终止工作相关的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的人工智能系统。

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) 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；

(d) 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。

6.执法，只要相关欧盟或成员国法律允许使用：

(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欧盟机构、机关、办公室或专业机构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) 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欧盟机构、机关、办公室或专业机构使用的人工智能系统，如测谎仪和类似工具；

(c) 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欧盟机构、机关、办公室或专业机构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；

(d) 供执法机关或代表执法机关使用的人工智能系统，或供支持执法机关或代表执法机关的欧盟机构、机关、办公室或专业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 段所述的自然人画像，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；

(e) 在侦查、调查或起诉刑事犯罪的过程中，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欧盟机构、机关、办公室或专业机构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，只要相关欧盟或成员国法律允许使用：

(a) 供主管公共机关用作测谎仪和类似工具的人工智能系统；

(b) 供主管公共机关或欧盟机构、办公室或专业机构或代表它们使用，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的人工智能系统；

(c) 供主管公共机关或欧盟机构、办公室或专业机构或代表它们使用，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的人工智能系统；

(d) 在移民、庇护和边境管制管理场景下，供主管公共机关或欧盟机构、办公室或专业机构或其代表使用，目的是检测、识别或辨认自然人的人工智能系统，但核查旅行证件除外；

8.司法和民主进程的管理：

(a) 拟由司法机关或其代表使用，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，或以类似方式用于替代性争议解决的人工智能系统;

(b) 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、优化和组织政治运动的工具。

附件四

第 11 条第 1 段提及的技术文件

第 11 条第 1 段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

⑷ 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）；

⑸ 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；

⑹ 相关软件或固件的版本以及与版本更新有关的任何要求；

⑺ 说明人工智能系统投放市场或提供服务的所有形式，例如嵌入硬件的软件包、可下载的软件包、 API 等；

⑻ 拟在其上运行人工智能系统的硬件的描述;

⑼ 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；

⑽ 向部署者提供的用户界面的基本描述；

⑾ 部署者的使用说明，以及在适用情形下向部署者提供的用户界面的基本说明；

2.详细描述人工智能系统的要素及其开发过程，包括：

⑷ 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；

⑸ 系统的设计规范，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；为遵守第三章第 2 节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；

⑹ 系统架构的说明，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；

⑺ 在相关的情况下，描述培训方法和技术以及所使用的培训数据集的数据表方面的数据要求，包括对这些数据集的一般描述、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的；打标签程序(如监督学习)、数据清理方法(如异常值检测)；

⑻ 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 段第⑷项评估所需的便于部署者解释人工智能系统的输出结果的技术措施；

⑼ 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章第 2 节规定的相关要求而采取的技术解决方案有关的所有信息；

⑽ 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章第 2 节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⑹点所述的预先确定的更改，须注明日期并由负责人签字。

⑾ 已部署的网络安全措施。

3.关于人工智能系统的监测、功能和控制的详细信息，特别是关于：其能力和性能限制，包括系统拟用于特定人员或人群的准确性程度，以及与预期目的相关的总体预期准确性水平；

鉴于人工智能系统的预期目的，对健康和安全、基本权利和歧视的可预见的意外后果和风险来源；根据第 14 条所需的人为监督措施，包括为促进部署人员解释人工智能系统输出而实施的技术措施；在适用情形下的输入数据的规范

4. 描述特定人工智能系统的性能指标的适当性；

5.根据第 9 条对风险管理系统的详细描述；

6.描述提供者在系统生命周期内对系统所做的相关更改；

7. 已在《欧盟官方公报》上公布的全部或部分适用的统一标准清单；如未采用此类统一标准，应详细说明为满足第三章第 2 节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；

8.第 47 条所述的欧盟合格性声明副本；

9.详细描述根据第 72 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 72 条第 3 段所述的后市场监测计划。

附件五

欧盟合格性声明

第 47 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，或在适用情形下的其授权代表的姓名和地址；

3.第 47 条所述的欧盟合格性声明由提供者全权负责签发的声明；

4.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第 47 条所述的欧盟合格性声明的相关欧盟立法的声明；

5.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(EU) 2016/679 条例、(EU) 2018/1725 条例和 (EU) 2016/680 指令。

6.所使用的声明与其相符的任何相关统一标准或任何其他共同规格的参考文件；

7.在适用的情况下，提供被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；

8.声明的签发地点和日期、签署人的姓名和职务，以及签署人的签名或其代表的签名。

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、3、4 点的合格性评估程序。

2.提供者核查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章第 2 节规定的相关基本要求。

4.提供者还核查人工智能系统的设计和开发过程以及第 72 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被通知机构提交过同一申请。

3.2.被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.提供者应将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提请被通知机构加以注意。
被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。
被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被通知机构提出申请，要求对与提供者意图投放市场或提供服务的人工智能系统有关的、属于第 3 点所述质量管理系统的范围的技术文件进行评估。

4.2.申请应包括
(a) 提供者的名称和地址；
(b) 一份书面声明，表明未向任何其他被通知机构提交过同一申请；

(c) 附件四提及的技术文件。

4.3.技术文件应由被通知机构审查。在相关和仅限于完成任务所必需的情况下，应允许被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， 被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章第 2 节的要求。如果被通知机构对提供者进行的测试不满意， 被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章第 2 节规定的要求，在已经用尽所有其他合理的核查合格性的方法并证明其不充分之后，如有必要，经确有依据据的请求，还应允许被通知机构查阅人工智能系统的训练过程和训练完成的模型，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.通知机构的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章第 2 节规定的要求，被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章第 2 节规定的要求，被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，被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，都应得到颁发欧盟技术文件评估认证的被通知机构的批准。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，通知上述被通知机构。被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 段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，被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，则应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 点中提及的被通知机构进行监督，其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，提供者应允许被通知机构进入设计、开发和测试人工智能系统的场所。提供者还应与被通知机构共享所有必要信息。

5.3.被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。在这些审计的场景中，被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 49 条登记高风险人工智能系统时提交的信息

A 节 根据第 49 条第 1 段登记高风险人工智能系统时提交的信息

对根据第 49 条第 1 段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.在适用的情形下，授权代表的姓名、地址和联系方式；

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额外明确参考；

5.对人工智能系统的预期目的以及该人工智能系统支持的组件和功能的描述;

6.系统使用的信息（数据、输入）及其运行逻辑的基本简明描述。

7.人工智能系统的现状（投放市场，或投入服务；不再投放市场/投入服务，召回）；

8.被通知机构颁发的认证的类型、编号和到期日期，以及在适用情况下该被通知机构的名称或识别号码；

9.在适用情况下第 8 点所述认证的扫描件；

10.人工智能系统已投放市场、投入服务或在欧盟提供的所有欧盟成员国；

11.第 47 条提及的欧盟合格性声明副本；

12. 使用的电子说明；附件三第 1、6 和 7 点所述的执法和移民、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。

13.其他信息的网址（URL）（可选）。

B 节 根据第 49 条第 2 段登记高风险人工智能系统时提交的信息

对根据第 49 条第 2 段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；

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.在适用情况下授权代表的姓名、地址和联系方式；

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额外明确参考；

5.说明人工智能系统的预期用途；

6.根据第 6 条第 3 段规定的哪一条或哪几条，认为人工智能系统不是高风险系统；

7.对人工智能系统在第 6 条第 3 段规定的程序应用中被视为非高风险的理由进行简要总结；

8.人工智能系统的状态（投放市场，或投入服务；不再投放市场/投入服务；已召回）；

9. 人工智能系统已投放市场、投入服务或在欧盟提供的所有欧盟成员国。

C 节 根据第 49 条第 3 段登记高风险人工智能系统时提交的信息

对于根据第 49 条第 3 段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；

3.根据第 27 条进行的基本权利影响评估的结论摘要；

4.人工智能系统提供者在欧盟数据库中输入的网址（URL）；

5.根据(EU) 2016/679 条例第 35 条，或在适用情况下本条例第 26 条第 8 段规定的(EU) 2016/680 指令第 27 条进行的数据保护影响评估的摘要。

附件九

附件三所列高风险人工智能系统登记时提交的关于按照第60条在真实世界进行测试的信息

根据第60条规定，应提供并不断更新在真实世界条件下进行测试的信息：

1. 在真实世界条件下测试的欧盟范围内唯一的单一识别号码；

2.在真实世界条件下参与测试的提供者或潜在提供者及部署者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. 在现实世界条件下测试计划的主要特征的总结；

5. 在真实世界条件下暂停或终止测试的信息。

附件十

欧盟关于自由、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(EU) 2018/1860 条例（官方公报，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，修订《申根协定实施公约》，并修订和废止(EC) No 1987/2006 条例的(EU) 2018/1861 条例（官方公报，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，并修订理事会 2007/533/JHA 号决定，并废止欧洲议会和欧盟理事会(EC) No 1986/2006 条例和欧盟委员会 2010/261/EU 号决定的(EU) 2018/1862 条例（官方公报，312，2018 年 12 月 7 日，第 56 页）。

2.签证信息系统

(a) 欧洲议会和欧盟理事会 2021 年 7 月 7 日有关为签证信息系统目的设置访问其他欧盟信息系统的条件，并修订(EU) No 603/2013 条例、(EU) 2016/794 条例、 (EU) 2018/1862 条例 (EU) 2019/816 和 (EU) 2019/818 条例的(EU) 2021/1133 条例（官方公报，248，2021 年 7 月 13 日，第 1 页）。

(b) 欧洲议会和欧盟理事会 2021 年 7 月 7 日出于改革签证信息系统的目的，并修订(EC) No 767/2008 条例、 (EC) No 810/2009 条例、(EU) 2016/399 条例、(EU) 2017/2226 条例、(EU) 2018/1240 条例、(EU) 2018/1860 条例、(EU) 2018/1861 条例、(EU) 2019/817 条例和(EU) 2019/1896 条例，并废止理事会 2004/512/EC 号和 2008/633/JHA 号决定的(EU) 2021/1134 条例（官方公报，248，2021 年 7 月 13 日，第 11 页)。

3.生物识别数据库（Eurodac）

欧洲议会和理事会 2024 年 5 月 14 日(EU)2024/1358 条例，关于为有效适用欧洲议会和理事会第(EU)2024/1315 条例和(EU)2024/1350 条例以及理事会 2001/55/EC 指令，并识别非法居留的第三国国民和无国籍人士，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(EU)2018/1240 条例和(EU) 2019/818 条例，废止欧洲议会和欧盟理事会(EU) No 603/2013 条例。（官方公报，2024/1258，2024 年 5 月 22 日，ELI: http://data.europa.eu/eli/reg/2024/1358/oj)。

4.出入境系统

欧洲议会和欧盟理事会 2017 年 10 月 30 日建立出入境系统，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，并确定为执法目的访问出入境系统的条件， 并修正《申根协定实施公约》以及(EU) 767/2008 条例和(EU)1077/2011 条例的(EU) 2017/2226 条例（官方公报，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，并修订(EU) 1077/2011 条例、(EU) 515/2014 号条例、(EU) 2016/399 条例、(EU) 2016/1624 条例和(EU) 2017/2226 条例的 2018/1240 号条例（官方公报，236，2018 年 9 月 19 日，第 1 页）。

(b) 欧洲议会和欧盟理事会 2018 年 9 月 12 日旨在建立欧洲旅行信息和授权系统，并修订了 2016/794 号条例的(EU) 2018/1241 条例（官方公报，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

欧洲议会和欧盟理事会 2019 年 4 月 17 日建立一个中央系统，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，以补充欧洲犯罪记录信息系统，并修订(EU) 2018/1726 条例的 2019/816 号条例（官方公报，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(EU)2019 /817 条例（官方公报，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(EU)2019/818 条例（官方公报，135，2019 年 5 月 22 日，第 85 页）。

附件十一

第53条第1段第(a)项所述的技术文件——通用人工智能大模型提供者的技术文档

第1节
所有通用人工智能大模型提供者应提供的信息

第53条第1段第(a)点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.通用人工智能大模型的一般性描述，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) 许可证；

2.详细描述第1段所述模型的要素，以及开发过程的相关信息，包括以下要素：

(a) 将通用人工智能大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，以及在适用情形下不同参数的相关性；

(c) 用于培训、测试和验证的数据信息，包括在适用情形下数据类型和来源、整理方法（如清洗、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，以及在可适用的情形下，检测数据源不适合性的所有其他措施和检测可识别偏见的方法；

(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) 模型已知或估计的能耗。

有关第(e)点，如果不知道模型的能耗，可根据所消耗计算资源的信息来确定。

第 2 节
具有系统性风险的通用人工智能大模型提供者应提供的补充信息

1. 评估策略的详细描述，包括基于现有公共评估协议和工具或其他评估方法的评估结果。评价策略应包括评价标准、度量标准和确定局限性的方法。

2. 在适用的情况下，详细描述为进行内部及/或外部对抗性测试(例如红队)、模型调整(包括校准和微调)而实施的措施。

3. 在适用的情况下，对系统架构的详细描述，解释软件组件如何构建或相互反馈，以及如何集成到整个过程中。

附件十二

第 53 条第 1 段第(b)项提及的透明度信息 ——通用人工智能大模型提供者提供技术文档，以便下游提供者将大模型集成到其人工智能系统中

第 53 条第 1 段第(b)项所述信息应至少包含以下内容：

1.通用人工智能大模型的一般描述，包括

(a) 大模型意图执行的任务，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) 大模型如何与不属于大模型本身的硬件或软件进行交互或可用于与之交互；

(e) 在适用情形下与使用通用人工智能大模型有关的相关软件版本；

(f) 结构和参数数量；

(g) 输入和输出的模态（如文本、图像）和格式；

(h) 大模型的许可证；

2.模型要件及其开发过程的说明，包括

(a) 将通用人工智能大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（如上下文窗宽等）；

(c) 在适用情形下用于训练、测试和验证的数据信息，包括数据的类型和来源以及保存方法。

附件十三

认定第 51 条所述的具有系统风险的通用人工智能大模型的标准

为确定通用人工智能大模型是否具有与第 51 条第 1 段第(a)项等价的能力或影响，欧盟委员会应考虑以下标准：

(a) 模型的参数数量；

(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，以浮点运算数衡量，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）、文本到图像和多模态，以及确定每种模式的高影响能力的先进水平阈值，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，包括考虑无需额外训练的适配任务数量、学习新的独特任务的可适应性、其自主程度和可扩展性、可使用的工具；

(f) 该产品是否因其覆盖范围而对内部市场产生较大影响，当该产品已提供给至少 10,000 个在欧盟设立的注册商业用户时，即推定该产品具有较大影响；

(g) 注册的终端用户数量。