

外国著作権法令集(63)

- EU AI 規則 編 -

前 文

井奈波 朋子 訳

March 2025

公益社団法人 著作権情報センター

目次

(1)	8
(2)	8
(3)	8
(4)	9
(5)	9
(6)	9
(7)	9
(8)	10
(9)	10
(10)	12
(11)	12
(12)	13
(13)	14
(14)	14
(15)	14
(16)	14
(17)	15
(18)	15
(19)	16
(20)	17
(21)	17
(22)	17
(23)	18
(24)	18
(25)	20
(26)	20
(27)	20
(28)	21
(29)	22
(30)	23
(31)	23
(32)	24
(33)	24
(34)	25
(35)	26

(36)	26
(37)	26
(38)	27
(39)	27
(40)	28
(41)	28
(42)	28
(43)	29
(44)	29
(45)	29
(46)	30
(47)	30
(48)	31
(49)	32
(50)	32
(51)	32
(52)	32
(53)	34
(54)	36
(55)	36
(56)	37
(57)	37
(58)	38
(59)	39
(60)	40
(61)	41
(62)	41
(63)	42
(64)	42
(65)	43
(66)	43
(67)	44
(68)	45
(69)	45
(70)	45
(71)	46

(72)	46
(73)	47
(74)	47
(75)	49
(76)	49
(77)	50
(78)	51
(79)	51
(80)	52
(81)	52
(82)	52
(83)	53
(84)	53
(85)	53
(86)	54
(87)	54
(88)	54
(89)	54
(90)	55
(91)	55
(92)	55
(93)	56
(94)	56
(95)	56
(96)	57
(97)	58
(99)	59
(100)	59
(101)	59
(102)	59
(103)	60
(104)	60
(105)	61
(106)	61
(107)	61
(108)	62

(109)	62
(110)	63
(111)	64
(112)	65
(113)	65
(114)	65
(115)	66
(116)	66
(117)	67
(118)	67
(119)	68
(120)	68
(121)	69
(122)	70
(123)	70
(124)	70
(125)	70
(126)	71
(127)	71
(128)	71
(129)	71
(130)	72
(131)	72
(132)	73
(133)	74
(134)	75
(135)	75
(136)	76
(137)	76
(138)	76
(139)	77
(140)	78
(141)	78
(142)	79
(143)	80
(144)	81

(145)	81
(146)	81
(147)	81
(148)	82
(149)	83
(150)	83
(151)	84
(152)	84
(153)	84
(154)	84
(155)	85
(156)	85
(157)	86
(158)	86
(159)	87
(160)	88
(161)	88
(162)	88
(163)	89
(164)	89
(165)	90
(166)	90
(167)	91
(168)	91
(169)	91
(170)	91
(171)	92
(172)	92
(173)	92
(174)	93
(175)	93
(176)	94
(177)	94
(178)	94
(179)	95
(180)	95

2024年4月16日

人工知能に関する統一ルールを定め、かつ
規則(EC)No 300/2008、(EU)No 167/2013、(EU)No 168/2013、(EU)2018/858、(EU)2018/1139 およ
び(EU)2019/2144 ならびに指令 2014/90 / EU、(EU)2016/797 および(EU)2020/1828 を
改正する欧州議会および欧州理事会規則(EU)2024/1689(人工知能規則)
を採択するため、2024年3月13日に第1読会において採択された欧州議会の見解に対する

訂正書

P9_TA(2024)0138

(COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

欧州議会の議事規則第241条に従い、上記の見解は、以下のとおり訂正される：

人工知能に関する統一ルールを定め、かつ
規則(EC)No 300/2008、(EU)No 167/2013、(EU)No 168/2013、(EU)2018/858、(EU)2018/1139 およ
び(EU)2019/2144 ならびに指令 2014/90 / EU、(EU)2016/797 および(EU)2020/1828 を
改正する欧州議会と欧州理事会規制(EU)2024/1689 (人工知能規則)

(欧州経済領域関連文書)

欧州議会および欧州理事会は、
欧州連合の機能に関する条約、特にその第16条および第114条に鑑み、
欧州委員会の提案を考慮し、
各国の国会に法案を回付した後、
欧州経済社会評議会の意見を考慮し¹、
欧州中央銀行(ECB)の意見を考慮し²、

¹ OJ C (欧州連合官報告示) 517, 22.12.2021, p56

² OJ C (欧州連合官報告示) 115, 11.3.2022, p5

地域委員会の意見を考慮し³、
通常の立法手続きに従って制定する⁴

理由は次のとおりである：

³ OJ C (欧州連合官報告示) 97, 28.2.2022, p60

⁴ 2024年3月13日の欧州議会の見解

- (1) 本規則の目的は、特に、EU の価値観に従って、EU 域内における人工知能システム(以下、「AI システム」という)の開発、上市、サービス開始および使用のための統一的な法的枠組みを定めることにより、域内市場の機能を向上させること、健康、安全、ならびに民主主義、法の支配および環境保護を含む、欧州連合基本権憲章(以下、「憲章」という)に記されている基本的権利のハイレベルな保護を保証しつつ、人間を中心とする信頼できる人工知能(AI)の採用を促進すること、EU 域内において AI システムの有害な影響から保護すること、イノベーションを支援することである。本規則が明示的に認めない限り、本規則は、加盟国が AI システムの開発、商品化および使用に制限を課すことを防止することにより、AI に基づく商品およびサービスの国境を越えた自由な移動を保証する。
- (2) 本規則は、自然人、企業、民主主義、法の支配および環境保護を促進し、イノベーションおよび雇用を刺激し、かつ EU を信頼できる AI の採用におけるリーダーにするものとして、憲章に記されている EU の価値観に従って適用されなければならない。
- (3) AI システムは、国境を越える場合を含む、経済の幅広い分野や社会の多くの面に容易に展開でき、かつ EU 域内全体に容易に流通し得る。一定の加盟国は、AI が信頼できる安全なものとなるように、かつ、基本的権利に関する義務に従って、AI が開発されおよび使用されるように確保するため、国内ルール of 採択を既に検討している。国内ルールが異なることは、域内市場の分断をもたらす可能性があり、かつ AI システムを開発し、輸入または使用するオペレータにとって法的安全を低下させる可能性がある。したがって、信頼できる AI を実現するため、かつ、域内市場において AI システムならびに関連する製品およびサービスの自由な移動、イノベーション、導入、および採用を妨げる相違を回避するため、オペレータに同じ義務を課すこと、および欧州連合の機能に関する条約(TFEU)第 114 条に基づき、域内市場全体において公共の利益と市民の権利という最優先の前提の統一的保護を保証することによって、EU 域内全体において、一貫したハイレベルな保護が保証されるべきある。個人データ処理、すなわち、法の執行を目的とした遠隔生体認証のための AI システムの使用の制限、法の執行を目的とした自然人に関するリスク評価のための AI システムの使用の制限、および法の執行を目的とした生体分類の AI システムの使用の制限に関する、本規則が個人の保護に特有のルールを含む範囲において、本規則は、これらの特有のルールに関する限り、TFEU 第 16 条に立脚することが適切である。これらの特有のルールを考慮し、かつ TFEU 第 16 条によることを考慮し、欧州データ保護委員会に諮問することが適切である。

- (4) AIは、産業や社会活動の分野全般にわたり、経済、環境、社会の幅広い利益に貢献する、急速に発展する技術系統である。AIの使用は、よりよい予測を提供すること、リソースの運用と配分を最適化すること、および個人や組織が利用できるデジタルソリューションをパーソナライズすることにより、例えば、ヘルスケア、農業、食品安全、教育および職業訓練、メディア、スポーツ、文化、インフラ管理、エネルギー、輸送と物流、公共サービス、安全保障、司法、資源とエネルギーの効率性、環境モニタリング、生物多様性と生態系の保全と回復、および気候変動の緩和と適応などの領域において、企業に対し決定的な競争上の優位性を提供することができ、社会および環境に対する有益な成果をもたらし得る。
- (5) 同時に、AIは、その具体的適用、使用および技術開発レベルに関する状況により、EU法により保護される公共の利益および基本的権利に対するリスクを生じさせ、害をもたらし得る。この害は、身体的、心理的、社会的、または経済的な害を含む、有形または無形のものであり得る。
- (6) AIがわれわれの社会に与え得る多大な影響と信頼構築の必要性を考慮し、AIおよびその規制のフレームワークは、欧州連合条約(TEU)第2条に記されているEUの価値観、条約に定める基本的権利および自由に従って、ならびにTEU第6条、憲章に従って、作成されることが不可欠である。前提条件として、AIは人間を中心とする技術でなければならない。AIは、人間の幸福を高めることを究極の目的とし、人々のためのツールとして供されるべきである。
- (7) 健康、安全、基本的権利に関する公共の利益の一貫したハイレベルな保護を確保するため、ハイリスクAIシステムに関する共通ルールを確立しなければならない。これらのルールは、憲章に従ったものであり、非差別的であり、EUの国際貿易コミットメントに合致したものでなければならない。これらのルールは、「デジタルの10年に向けたデジタルの権利と原則に関する欧州宣言」、および人工知能に関するハイレベル専門家グループ(AIHLEG)による「信頼できるAIのための倫理ガイドライン」も、考慮しなければならない。

(8) したがって、AI に関する統一ルールを定める EU の法的枠組みは、健康および安全、ならびに EU 法により認められ保護されている民主主義、法の支配および環境保護を含む基本的権利の保護などの、公共の利益のハイレベルな保護を保証しつつ、域内市場における AI の開発、使用および採用を促進するために必要である。この目的を達成するため、域内市場の良好な機能を保証しつつ、かつ、これらのシステムが商品およびサービスの自由移動の原則を享受できるようにしつつ、一定の AI システムの上市、サービス開始および使用を規制するルールを定めなければならない。これらのルールは、基本的権利を保護するため、新たな革新的ソリューションを支援するため、EU の価値観に合致した AI システムを創造する官民行為者の欧州エコシステムを確立するため、かつ EU のあらゆる地域全体においてデジタルトランスフォーメーションの可能性を解放するため、明確かつ堅牢なものでなければならない。これらのルール、およびスタートアップを含む中小企業(SME)を特に重視したイノベーションのための措置を定めることにより、本規則は、人間を中心とする欧州の AI アプローチを促進するという目的、および欧州理事会が表明したように⁵、EU がセキュアで信頼できる倫理的な AI の開発における世界的リーダーになるという目的の実現に寄与し、欧州議会から特に求められている⁶倫理原則の保護を保証する。

(9) ハイリスク AI システムの上市、サービス開始、および使用に対して適用される統一ルールは、欧州議会および欧州理事会規則(EC)No765/2008⁷、欧州議会および欧州理事会決定 No 768/2008/EC⁸、ならびに欧州議会および欧州理事会規則(EU)2019/1020⁹(以下、「新たな立法枠組み」という)に従って定められなければならない。本規則に定める統一ルールは、あらゆる分野に、かつ新たな立法枠組みに従って、適用されなければならない。本規則が補完する、特にデータ保護、消費者保護、基本的権利、雇用および労働者保護、ならびに製品の安全性に関する既存の EU 法を害するものであってはならない。

その結果、欧州理事会指令 85/374/EEC¹⁰に従った損害賠償の可能性に関するものを含め、消費者および AI システムが悪影響を与え得るその他の者に対する、この EU 法が定めるあらゆる

⁵ 欧州理事会、欧州理事会特別会合(2020年10月1日および2日)–結論、EUCO 13/20、2020、p6。

⁶ 人工知能、ロボット工学、および関連技術の倫理的側面に対する枠組みに関する欧州委員会への勧告を含む 2020年10月20日の欧州議会決議、2020/2012(INL)。

⁷ 認証要件を定め、かつ欧州理事会規則(EEC)No 339/93 を廃止する 2008年7月9日の欧州議会および欧州理事会規則(EC)No 765/2008 (OJ L 218、13.8.2008、p.30)。

⁸ 製品の商品化のための共通の枠組みに関する、および欧州理事会決定 93/465/EEC を廃止する 2008年7月9日の欧州議会および欧州理事会決定 No768/2008/EC (OJ L 218、13.8.2008、p82)。

⁹ 製品の市場監視および適合性に関する、ならびに指令 2004/42 / EC および規則(EC)No 765/2008 および(EU)No 305/2011 を改正する 2019年6月20日の欧州議会および欧州理事会規則 (EU)2019/1020 (OJ L 169、25.6.2019、p.1)。

¹⁰ 欠陥製品に対する責任に関する加盟国の法律上、規則上、および行政上の規定の近接に関する 1985年7月25日の欧州理事会指令 85/374 / EEC(OJ L 210、7.8.1985、p.29)。

権利および救済は影響を受けることなく、完全に適用される。さらに、雇用と労働者の保護の文脈において、本規則は、労働における健康および安全、ならびに雇用者と労働者との関係を含む雇用条件および労働条件に関し、EU法の遵守において、社会政策に関するEU法に対しても国内労働法に対しても影響を与えるものであってはならない。また、本規則は、加盟国およびEUレベルで認められている基本的権利の行使、特に加盟国に特有の労使協議制度によって定められるストライキの権利または自由、その他の行動をとる権利または自由、ならびに労働協約を交渉し、締結しおよび執行する権利、または国内法に従って集団行動をとる権利の行使に、影響を与えるものであってはならない。

本規則は、プラットフォーム労働における労働条件の改善に関する欧州議会および欧州理事会の指令に定める、プラットフォーム経由の労働の枠内における労働条件の改善を目的とする規定に影響を与えるものであってはならない。さらに、本規則は、AIシステムの透明性、技術文書および記録保持に関するものを含め、特別の要件および義務を定めることにより、これらの既存の権利および救済の有効性を強化することを目的とする。加えて、本規則に基づきAIバリューチェーンに関与するさまざまなオペレータに課せられる義務は、EU法に従って、これら国内法の規定が本規則の適用範囲外である場合、または、本規則で追求されるものとは別の正当な公益目的を追求する場合、一定のAIシステムの使用を制限する効果を有する国内法を害することなく適用されなければならない。したがって、国内労働法、および未成年者、すなわち18歳未満の者の保護法は、デジタル環境における子どもの権利に関するUNCRCのジェネラル・コメント第25号(2021年)を考慮し、AIシステムに特有のものでなく、かつ、他の正当な公益目的を追求するものである限り、本規則の影響を受けるものであってはならない。

- (10) 個人データの保護に対する基本的権利は、特に欧州議会および欧州理事会規則(EU)2016/679¹¹ および(EU)2018/1725¹²、ならびに欧州議会および欧州理事会指令(EU)2016/680¹³によって保証される。さらに、欧州議会および欧州理事会指令 2002/58/EC¹⁴は、端末機器への個人データおよび非個人データの保存のための条件、ならびにこれらの機器からこれらのデータへアクセスする条件を定めること含む、プライバシーおよび通信の機密を保護する。これらの EU 法は、データセットに個人データと非個人データが混在している場合を含め、サステイナブルでかつ責任あるデータ処理の基礎を提供する。本規則は、個人データ処理を定める既存の EU 法の適用を修正するものではなく、これらの法律の遵守を確保することを任務とする独立の監督当局の任務および権限を修正するものでもない。

これは、また、AI システムの設計、開発、または使用が個人データ処理を前提とする限り、個人データの保護に関する EU 法または国内法から生じるデータ管理者または処理者としての役割にある AI システムの提供者および導入者の義務に影響を与えるものでもない。また、データ主体は、EU 法によってデータ主体に付与されたすべての権利と保証を引き続き享受するが、その権利には、プロファイリングを含む、完全に自動化された個人の意思決定に関連する権利を含むことを明確にすることも適切である。本規則に基づき定められる AI システムの上市、サービス開始および使用に関する統一ルールは、個人データ保護およびその他の基本的権利に関する EU 法により保証される権利およびその他の救済手段の効果的な実施を促進し、かつデータ主体に対しこれらの権利およびその他の救済手段の行使を可能にするものでなければならない。

- (11) 本規則は、欧州議会および欧州理事会規則(EU)2022/2065¹⁵に定める仲介サービス提供者の責任に関する規定を害しない。

¹¹ 個人データの処理における自然人の保護およびこれらのデータの自由な移動に関する、ならびに指令 95/46/EC を廃止する 2016 年 4 月 27 日の欧州議会および欧州理事会規則(EU)2016/679(一般データ保護規則)(OJ L 119, 4.5.2016, p.1)。

¹² EU の機関、組織、部署および事務所による個人データ処理における自然人の保護およびこれらのデータの自由な移動に関する、ならびに規則(EC)No 45/2001 および決定 No 1247/2002/EC を廃止する 2018 年 10 月 23 日の欧州議会および欧州理事会規則(EU)2018/1725 (OJ L 295, 21.11.2018, p39)。

¹³ 刑事犯罪の防止、探知、捜査および訴追、または刑事罰の執行を目的とした管轄当局による個人データ処理における自然人の保護、およびこれらのデータの自由な移動に関する、ならびに欧州理事会の枠組み決定 2008/977/JHA を廃止する 2016 年 4 月 27 日の欧州議会および欧州理事会指令(EU)2016/680 (OJ L 119, 4.5.2016 年 5 月 4 日, p89)。

¹⁴ 電気通信分野における個人データの処理およびプライバシーの保護に関する 2002 年 7 月 12 日の欧州議会および欧州理事会指令 2002/58/EC (プライバシーおよび電子通信指令)(OJ L 201, 31.7.2002, p37)。

¹⁵ デジタルサービスの単一市場に関する、および指令 2000/31/EC を改正する 2022 年 10 月 19 日の欧州議会および欧州理事会規則(EU) 2022/2065 (デジタルサービス規則)(OJ L 277, 27.10.2022, p.1)。

(12) 本規則という「AI システム」の概念は、この分野における急速な技術的發展に対応するために必要な柔軟性を示しつつ、法的安全を保証するため、かつ国際的な見解の一致および幅広い支持を得るために、明確に定義されなければならない、かつ AI 分野に取り組む国際機関の成果とほぼ一致するものでなければならない。さらに、この定義は、より簡単な従来のソフトウェアシステムやプログラミングアプローチから AI システムを区別する、AI システムの本質的な特徴に基づくべきであり、かつ自動的に操作を実行するように自然人によってのみ定義されたルールに基づくシステムを対象とすべきではない。AI システムの本質的な特徴は、その推論能力である。この推論能力とは、現実の環境や仮想の環境に影響を与え得る予測、コンテンツ、提言または判断などの出力を生成するプロセスと、入力やデータから、モデルやアルゴリズム、またはその双方を推論する AI システムの能力をいう。AI システムの構築において推論を可能とする技術には、ある目的を達成する方法をデータから学習する機械学習アプローチと、コード化された知識または解決すべきタスクの記号表現から推論する論理ベースおよび知識ベースのアプローチとを含む。AI システムの推論能力は、基本的なデータ処理を超えて、学習、推論、モデリングを可能にする。「マシンベース」という用語は、AI システムがマシン上で動作することを意味する。

明示または黙示の目的という用語は、AI システムが明示的に定義された目的に従い、または黙示の目的に従い、動作し得ることを強調する。AI システムの目的は、特定のコンテキストにおける AI システムの意図目的とは異なる場合がある。本規則の目的上、環境とは、AI システムが動作するコンテキストをいい、これに対し、AI システムによって生成される出力は、AI システムが実行するさまざまな機能に対応し、予測、コンテンツ、提言または判断で構成される。AI システムは、さまざまなレベルの自律性において動作するように設計されているが、これは、AI システムが人間の干渉からのある程度の独立性を有し、かつ人間の介入なく動作する能力を有することを意味する。AI システムがその導入後に示し得る適応性は、使用中にシステムの変更が可能な自己学習能力に関連する。AI システムは、スタンドアロンベースで使用されることも、製品のコンポーネントとして使用されることもあり、それはシステムが製品に物理的に内蔵されているか(搭載)か、製品に内蔵されることなく製品の機能に役立つか(非搭載)を問わない。

- (13) 本規則にいう「導入者」の概念は、公的機関、事務所、またはその他の組織を含む、その権限の下でAIシステムを使用するすべての自然人または法人であり、AIシステムが事業性のない個人的な活動の範囲内において使用される場合を除くものとして解釈されることが適切である。AIシステムの種類によっては、そのシステムの使用は導入者以外の者に関係することがある。
- (14) 本規則において用いられる「生体データ」の概念は、規則(EU)2016/679 第4条(14)、規則(EU)2018/1725 第3条(18)、および指令(EU)2016/680 第3条(13)において定義される生体データの概念に照らし、解釈されることが適切である。生体データは、自然人の認証、識別または分類、および自然人の感情の認識を可能とする。
- (15) 本規則にいう「生体認証」の概念は、本人が同意を与えたか否かを問わず、参照データベースに保存されている人の生体データとその人の生体データとを比較することにより、人の識別を行う目的で、顔、眼球運動、体型、声、抑揚、歩き方、姿勢、心拍数、血圧、匂い、キーボードのタッチなど、人の身体的、生理的および行動的特徴を自動認識することと定義されるべきである。特定の自然人がそれと主張する本人であることを確認することのみを目的とする、およびサービスへのアクセス、デバイスのロック解除、または施設への安全なアクセスのみの目的で自然人の同一性を確認することのみを目的とする認証を含む、生体1対1認証に使用されることを目的とするAIシステムは、これから除かれる。
- (16) 本規則にいう「生体分類」の概念は、自然人の生体データに基づき、その自然人を一定の分類に割り当てることと定義されるべきである。これらの具体的分類は、性別、年齢、髪の色、目の色、入れ墨、行動または性格的特徴、言語、宗教、少数民族に属すること、性的または政治的指向などの側面に関連し得る。これには、他の商用サービスに内在的に結び付けられる、純粹に付随的な特性である生体分類システムは含まない。つまり、この特性は、客観的に技術的理由により、主たるサービスなくして使用され得ないこと、および、この特性または機能を統合することが、本規則のルール適用の可能性を回避する手段ではないことを意味する。例えば、オンラインマーケットプレイスで使用される顔や体の特性を分類するフィルターは、消費者が自分自身で商品のディスプレイをプレビューし、購入の判断を下すことを助けることを可能にすることにより、商品を販売することから成る、主たるサービスに関連してのみ使用され得るものであるから、その付随的な特性を構成するものといえる。ユーザーが写真やビデオを追加または変更することができるように顔や体の特性を分類する、オンラインソーシャルネットワークサービス上で使用されるフィルターも、この種のフィルターはオンラインでのコンテンツの共有からなるソーシャルネットワークサービスの主たるサービスなく使用され得ないものであるから、付随的な機能とみなすことができる。

- (17) 本規則にいう「遠隔生体認証システム」の概念は、使用される生体データ特有の技術、プロセスまたは種類を問わず、個人の生体データと参照データベース内にある生体データとを比較することにより、自然人が能動的に関与することなく、通常は遠隔で、自然人を識別することを目的とする AI システムとして、機能的に定義されるべきである。これらの遠隔生体認証認識システムは、通常、自然人が能動的に関与することなく、自然人の識別を著しく容易にする目的で、複数の人またはその行動を同時に把握するために使用される。特定の自然人がそれと主張する本人であることを確認することのみを目的とする、およびサービスへのアクセス、デバイスのロック解除、または施設への安全なアクセスのみの目的で自然人の同一性を確認することのみを目的とする認証を含む、生体 1 対 1 認証に使用されることを目的とする AI システムは除かれる。この除外は、このシステムが、自然人が能動的に関与することなく、大勢の人の生体データ処理のために使用され得る遠隔生体認証システムと比べ、自然人の基本的権利に対して与え得る影響が軽微であるという事実によって、正当化される。「リアルタイム」システムの場合、生体データの取得、比較および識別は、まったくの瞬時、ほぼ瞬時、またはいかなる場合も大きな時間的格差なく行われる。この点に関し、軽微な時間的格差の可能性を定めることにより、関係する AI システムの「リアルタイム」の使用について、本規則のルールを回避する余地があってはならない。「リアルタイム」システムは、カメラまたは同様の機能を持つ他のデバイスによって作成されたビデオ映像などの「ライブ」または「ニアライブ」素材の使用を前提とする。これに対し、「事後的」システムの場合、生体データは既に取得され、かつ、比較および識別は、大幅な遅れの後にのみ行われる。これは、関係する自然人に対する、システムを使用する前の、CCTV や私的なデバイスによって作成された画像やビデオ映像などの素材を前提とする。
- (18) 本規則にいう「感情認識システム」の概念は、自然人の生体データに基づき、その自然人の感情または意図を識別または推測することを目的とする AI システムと定義されるべきである。この概念は、幸せ、悲しみ、怒り、驚き、嫌悪、困惑、興奮、恥かしさ、軽蔑、満足、楽しさなどの感情または意図をいう。この概念には、例えば、事故防止の目的でプロのパイロットやドライバーの疲労状態を検知するために使用されるシステムを含む、痛みや疲労のような、身体的状態を対象としない。この概念は、直ちにはっきりする表情、しぐさまたは動作の単なる検知も、それらが感情の識別や推測に使用される場合を除き、対象としない。これらの表現は、眉をひそめたり微笑んだりするなどの単なる顔の表現、または手、腕、頭の動きなどのしぐさ、さらには大声を上げたりささやいたりするなどの人の声の特徴もあり得る。

- (19) 本規則における、「公衆がアクセス可能な場所」の概念は、不特定数の自然人がアクセス可能なあらゆる物理的場所を意味するものと理解され、問題の場所が私有か公有かを問わず、商取引のための、たとえば店舗、レストランまたはカフェなど、サービス提供のための、たとえば銀行、専門職の活動またはホテルなど、スポーツ活動のための、たとえばプール、ジムまたはスタジアム、輸送のための、たとえば、バス停留所、地下鉄の駅および鉄道の駅、空港または他の交通手段、娯楽のための、たとえば、映画館、劇場、博物館、コンサートホールまたは会議場、またはレジャーやその他のための、たとえば、道路および広場、公園、森林、遊び場のような、その場所が使用されることになる活動には無関係である。また、収容人数やセキュリティ制限を問わず、アクセスが、チケット購入や交通手段の購入、事前登録または一定の年齢である事実など、不特定数の人によって満たされ得る一定の条件に従う場合、ある場所は公衆がアクセス可能であると分類される。これに対し、公共の安全またはセキュリティに直接的に関係する EU 法もしくは国内法のいずれかによって定められた、またはその場所に関連する権限がある者の明確な意思表示によって定められた、一定の自然人にアクセスが限定されている場合、ある場所は公衆がアクセス可能であるとは見なされない。アクセスの禁止または制限の標識のように、公衆がアクセス可能でないことを示唆する表示または状況が存在する、施錠されていないドアや囲いにある開いた門など、アクセスの可能性があるという事実だけでは、その場所が公衆によりアクセス可能であることを意味しない。企業および工場の敷地、ならびに関係する従業員やサービス提供者のみのアクセスを目的とする事務所や職場は、公衆がアクセス可能な場所ではない。公衆がアクセス可能な場所は、刑務所も出入国管理局も含まない。他のいくつかの場所は、診療所にアクセスするために通過しなければならない民間住宅の建物のホールや空港のホールなど、公衆がアクセス可能な場所と公衆がアクセス可能でない場所が併存する可能性がある。オンラインの空間は、物理的な場所でないため、対象とならない。ただし、当該場所について公衆がアクセス可能な性格であるか否かは、問題の状況の特性を考慮し、ケースバイケースで決定されなければならない。

- (20) 基本的権利、健康および安全を保護しつつ、AI システムから最大の利益を得るため、かつ民主的管理を可能にするため、提供者、導入者および関係者は、AI リテラシーの枠内において、AI システムに関し情報に基づいた決定を下すために、必要な概念を身に着けなければならない。これらの概念は、文脈により異なり得るものであり、AI システムの開発段階における技術的要素の正しい適用、その使用中に適用されるべき措置、AI システムの出力を解釈する適切な方法の理解、および関係者の場合、AI の支援を受けて行われた判断がどのように関係者に影響するかを理解するための必要な知識の理解が含まれる。本規則の適用の範囲内において、AI リテラシーは、適切なコンプライアンスおよびそれが正しく実行されることを保証するために、AI バリューチェーンにおけるすべての関係する行為者に対し、必要な見識を提供するものでなければならない。さらに、AI リテラシーに関する措置の広範な実施および適切なフォローアップ活動の導入は、労働条件の改善に寄与し得るものであり、最終的に EU 域内における信頼できる AI の強化およびイノベーションの道筋を支え得る。欧州人工知能委員会(以下「AI 委員会」という)は、AI リテラシーツール、公衆の注意喚起、ならびに AI システムの使用に関連する利益、リスク、セーフガード、権利および義務に関する理解の促進のために、欧州委員会を支援しなければならない。欧州委員会および加盟国は、関係するステークホルダーと協力し、AI の開発、操作および使用を担う者のもつて、AI リテラシーの向上のための自主的な行動規範の策定を促進しなければならない。
- (21) EU 域内全体における公平な競争条件、ならびに個人の権利および自由の効果的な保護を保証するために、本規則に定めるルールは、EU 域内において設立されたか第三国において設立されたかを問わず、AI システムの提供者に対し、および EU 域内で設立された AI システムの導入者に対し、非差別的な方法で適用されなければならない。
- (22) 一定の AI システムは、そのデジタルという性質を考慮し、EU 域内において、それが上市されていない場合、サービスが開始されていない場合、または使用されていない場合であっても、本規則の対象にしなければならない。特に、EU 域内において設立されたオペレータが、ハイリスクと見なされる AI システムによって実行されることになる活動に関連し、第三国において設立された外部オペレータに対し、一定のサービスの実施を委ねる場合がこれに該当する。これらの状況において、オペレータが第三国において使用する AI システムは、EU から合法的に収集されかつ移転されるデータを処理する可能性があり、この処理に由来する当該 AI システムの出力を、EU 域内において設立された契約相手のオペレータに対し、この AI システムを EU 域内において上市し、サービスを開始しまたは使用することなく、提供する可能性がある。本規則のルールを迂回することを回避し、かつ EU 域内に所在する自然人の効果的な保護を確保するために、本規則は、第三国で設立された AI システムの提供者および導入者に対しても同じく、これらのシステムの出力が EU 域内において使用されることを目的とする範囲において、適用されなければならない。

しかし、情報および証拠が交換される外国のパートナーとの将来の協力のための既存の取決め

および特別な必要性を考慮すると、関係する第三国または関係する国際機関が、人の自由および基本的権利の保護に関し適切なセーフガードを提供することを条件として、第三国または国際機関の公的機関が、EU または加盟国と法執行協力および司法協力のために EU レベルまたは加盟国レベルで締結した協力協定または国際協定の枠内で行動する場合、本規則は、第三国の公的機関にも国際機関の公的機関にも適用されるべきではない。必要に応じ、これは、この法執行協力および司法協力に基づき具体的な任務を遂行するために、第三国から委ねられた主体の活動を含みうる。このような協力または合意の枠組みは、加盟国と第三国の間、または欧州連合、ユーロポールと他の EU の事務所、第三国および国際機関との間の二国間で締結される。本規則に基づき法執行機関および司法当局を監督する管轄を有する当局は、これらの協力または国際合意の枠組みが、人の自由および基本的権利の保護に関する適切なセーフガードを含むものかどうかを評価しなければならない。受益者である国内当局、および EU 域内においてこれらの出力を使用する EU の機関、組織、部署および事務所は、その使用が EU 法を遵守していることを確保する責任者である。これらの国際合意の見直しまたは将来の新たな合意締結の際、契約当事者は、これらの合意を本規則の要件に合致させるため、最大限の努力をしなければならない。

- (23) 本規則は、EU の機関、組織、部署および事務所が AI システムの提供者または導入者として行動する場合、それらにも適用されなければならない。
- (24) AI システムが、軍事目的、防衛目的、または国家安全保障目的で、これらシステムの変更の有無にかかわらず、上市され、サービスが開始され、または使用される場合において、かつその範囲に限り、公的な者であるか私的な者であるかなど、これらの活動を行う者の種類を問わず、これらのシステムは、本規則の適用範囲から除外されなければならない。軍事目的および防衛目的の使用に関しては、当該除外は、TEU 第 4 条第 2 項によっても、軍事活動および防衛活動の枠内における致命的な武力および他の AI システムの使用の文脈での AI システムの規制のためのより適切な法的枠組みである国際公法の対象となる TEU 第 V 編第 2 章に挙げられる加盟国の防衛政策および EU の共通防衛政策の特殊性によっても、正当化される。国家安全保障の目的の使用に関しては、当該除外は、TEU 第 4 条第 2 項に従って、国家安全保障が各加盟国の単独の責任にとどまるという事実によっても、国家安全保障に関する特別の性質および作戦上の必要、ならびにこれらの活動に適用される特別な各国ルールによっても、正当化される。しかし、軍事目的、防衛目的、または国家安全保障の目的で、開発され、上市され、サービスが開始され、または使用される AI システムが、一時的または恒久的に、この枠外で別の目的で使用される場合（民生目的または人道的目的、法執行目的または公安目的など）、当該システムは、本規則の適用範囲に含まれることになる。

この場合、軍事目的、防衛目的、または国家安全保障の目的以外の目的で AI システムを使用する者は、システムが既に本規則に遵守している場合を除き、AI システムが本規則を遵守してい

ることを確保しなければならない。除外された目的、すなわち軍事目的、防衛目的または国家安全保障の目的で、および民生目的または法執行目的のような除外されていない1つ以上の目的で、上市されまたはサービスが開始された AI システムは、本規則の適用範囲に含まれ、これらのシステムの提供者は、本規則の遵守を確保しなければならない。これらの場合、AI システムが本規則の適用範囲に含まれ得るという事実は、国家安全保障活動、防衛活動および軍事活動を行う主体の種類にかかわらず、これらの活動を行う者が、その使用が本規則の適用範囲外である国家安全保障目的、軍事目的および防衛目的で AI システムを使用する可能性に影響を与えてはならない。民生目的または法執行目的で上市される AI システムで、軍事目的、防衛目的、または国家安全保障目的で変更の有無にかかわらず使用されるものは、これらの活動を行う者の種類にかかわらず、本規則の適用範囲に含まれない。

- (25) 本規則は、イノベーションを支援し、学術上の自由を尊重するものでなければならない。かつ研究開発活動を損なうものであってはならない。したがって、学術的な研究開発のみを目的として特別に開発され、かつサービスが開始された AI システムおよび AI モデルを、その適用範囲から除外することが必要である。さらに、本規則が、そのほか、その上市またはサービス開始前に、AI システムまたはモデルの学術的な研究開発活動に影響を与えないように確保することが必要である。AI システムまたは AI モデルに関する製品志向の研究、テスト、および開発活動についても、本規則の規定は、これらのシステムおよびモデルのサービス開始または上市前に適用されるべきではない。この除外は、本規則の適用範囲に含まれる AI システムが、この研究開発活動の結果、上市されまたはサービスが開始された場合に、本規則を遵守する義務を害するものではなく、かつ正規 AI サンドボックスおよびリアルワールドテストに関する規定の適用を害するものではない。さらに、学術的な研究開発のみを目的として特別に開発されかつサービスが開始された AI システムの除外を害することなく、研究開発活動を行うために使用され得るその他の AI システムは、そのまま本規則の規定の対象とされなければならない。いずれにせよ、あらゆる研究開発活動は、学術的な研究の分野において認められる倫理規範および職業規範に従って実施され、かつ適用される EU 法に従って実施されなければならない。
- (26) AI システムについて、相応で効果的な拘束力のある一連のルールを導入するため、明確に定義されたリスクベースのアプローチに従うことが適切である。当該アプローチでは、これらのルールの種類および内容を、AI システムが引き起こし得るリスクの大きさと範囲に適合させなければならない。したがって、AI に関して許容できない一定の行為を禁止し、ハイリスク AI システムの要件および関係するオペレータの義務を定め、かつ、一定の AI システムについて透明性の義務を定めることが必要である。
- (27) リスクベースのアプローチが、相応で効果的な拘束力のある一連のルールの基礎を構成するものであるとすれば、欧州委員会によって任命された独立した AI HLEG によって 2019 年に策定された信頼できる AI のための倫理ガイドラインに立ち返ることが重要である。これらのガイドラインにおいて、AI HLEG は、AI についての拘束力のない 7 つの倫理原則を策定し、これは AI が信頼でき倫理的に健全であることの確保に寄与することを目的とする。7 つの原則は、以下のとおりである：人間の活動と人間による監督；技術的な堅牢性と安全性；プライバシーの尊重とデータガバナンス；透明性；多様性、非差別性および公平性；社会的および環境的福祉；説明責任。本規則および適用されるその他の EU 法の法的拘束力のある要件を害することなく、これらのガイドラインは、憲章および EU が設立された価値観に従って、一貫した、信頼できる、人間を中心とする AI の構想に貢献する。AI HLEG のガイドラインに従えば、人間の行為と人間による監督は、AI システムが人に奉仕するツールとして開発されかつ使用されることを意味し、そして、それは人間の尊厳および個人の自律性を尊重するものであり、かつ、人間によって適切にコントロールされおよび監督されることができるように機能することを意味する。

技術的な堅牢性と安全性とは、AI システムが、問題に対して技術的に堅牢な方法で開発されかつ使用されること、ならびに第三者が違法な使用を可能にする使用やパフォーマンスを変更しようとする試みに対してレジリエンスを有する方法で、および意図しない侵害を最小限に抑える方法で開発されかつ使用されることを意味する。プライバシーの尊重とデータガバナンスとは、AI システムが、品質と完全性において高度な規格に合致するデータ処理の枠内において、プライバシーの尊重とデータ保護のルールに従って、開発および使用されることを意味する。透明性とは、人間が AI システムと意思疎通または交流していることを人がわかるようにしつつ、適切なトレーサビリティと説明可能性を可能にする方法により AI システムが開発および使用されること、導入者が、この AI システムの性能および限界について十分な情報を与えられること、および関係者がその権利について情報を与えられることを意味する。多様性、非差別性および公平性とは、EU 法または国内法により禁止される差別的結果および不公正なバイアスを回避しつつ、多様な行為者を包摂する方法で、かつアクセスの平等、ジェンダーの平等、文化的多様性を促進する方法で、AI システムを開発および使用することを意味する。社会的および環境的福祉とは、個人、社会および民主主義に対する長期的な影響を監視しおよび評価しつつ、AI システムが、サステイナブルなおよび環境に優しい方法により、およびすべての人間がそれから利益を得る方法により、開発および使用されることを意味する。これらの原則は、可能な限り、AI モデルの設計と使用において反映されなければならない。いずれにせよ、本規則に基づく行動規範の策定の基礎として役立つものでなければならない。産業界、学界、市民社会、標準化機関を含む、すべてのステークホルダーは、自主的なベストプラクティスおよび規格の策定に、倫理原則を考慮に入れることが奨励される。

- (28) AI が多くの有益な目的で用いられ得るとしても、AI は誤って用いられる可能性もあり、かつ、操作、悪用、社会統制の各行為のための新しい強力なツールを提供しうる。当該行為は、特に有害で濫用的であり、かつ人間の尊厳、自由、平等、民主主義および法の支配の尊重に関する、ならびに差別をうけない権利、データ保護に対する権利、プライバシーの権利および子どもの権利を含む、憲章に記されている基本的権利の尊重に関する、EU の価値観に反するとの理由により、禁止されなければならない。

(29) AI が可能とする操作技術は、望ましくない行動をとることを人々に仕向けるために、またはその自律性、自由な意思決定および選択の自由を否定しかつ損なうような方法で人々に判断を迫ることによって人々を誤らせるために用いられ得る。重大な害を引き起こすリスクを伴う、特に、心身の健康または金銭的利益に対し極めて重大な悪影響を与える、人間の行動を著しく歪曲する目的または効果を有する、一定の AI システムの上市、サービス開始または使用は、特に危険であり、したがって禁止されなければならない。これらの AI システムは、音声の、画像のまたは映像の刺激など、これらの刺激が人の知覚を越えるような、人が知覚できないサブリミナルコンポーネントを介在させたり、人の自律性、自由な意思決定、または選択の自由を否定しまたは歪曲するその他の操作的なまたは欺瞞的な他の技術で、これにより人はこれらの技術を意識せず、または、人がそれを知っていたとしても、欺瞞から逃れることもできず、当該技術に抵抗したりすることも制御することもできない技術を介在させたりする。これは、例えば、機械と脳とのインターフェースまたは仮想現実によって促進され得るものであるが、それは、それらが非常に有害な方法により人の行動を顕著に歪曲し得る限り、人に示される刺激をより高度にコントロールできるようになるからである。さらに、AI システムは、その年齢、欧州議会および欧州理事会指令 (EU)2019/882¹⁶にいう心身障害によって、または、極度の貧困状態にある人または民族的または宗教的マイノリティに属する人のように、悪用に対して人をより脆弱にし得る特定の社会的または経済的状況によって、人の脆弱性または人の特定のグループの脆弱性につけこむ可能性もある。

そのような AI システムは、人もしくは他の人または人のグループに対し、重大な害を引き起こし、または合理的に引き起こし得る方法で、人の行動を著しく歪曲する目的または効果をもって、上市され、サービスが開始され、または使用され得、それは時がたつにつれ、蓄積され得る害を含むものであり、したがって、それを禁止すべきである。この歪曲が、提供者または導入者のコントロールの及ばない AI システムの外部要因、すなわち合理的に予見し得ない要因であり、それゆえ AI システムの提供者または導入者が軽減できない要因から生じる場合、行動を歪曲する意図の存在を想定できない可能性がある。いずれにせよ、この害が AI を前提とする操作または悪用に起因するものである以上、提供者または導入者が重大な害を引き起こす意図を有することは必要ではない。AI に関するこのような行為の禁止は、欧州議会および欧州理事会指令 2005/29/EC¹⁷の規定を補完するものであり、特に、消費者に経済的または金銭的な損失をもたらす不公正な商慣行は、AI システムにより導入されるものか否かを問わず、あらゆる状況において禁止される。本規則に定める操作および悪用の禁止は、人またはその法定代理人の明示の同意がある場合のように、当該行為が適用される法および医療規範に従って行われる場合、精神疾患の心理的治療または身体的なリハビリテーションなどの医療の枠内においては、合法的な行為に影響

¹⁶ 製品およびサービスのアクセシビリティ要件に関する 2019 年 4 月 17 日の欧州議会および欧州理事会指令(EU)2019/882(OJ L 151, 7.6.2019, p.70)。

¹⁷ 域内市場における B to C の不公正な商慣行に関する、ならびに欧州理事会指令 84/450/EEC、欧州議会および欧州理事会指令 97/7/EC、98/27/EC、2002/65/EC、欧州議会および欧州理事会規則(EC)No 2006/2004 を修正する 2005 年 5 月 11 日の欧州議会および欧州理事会指令 2005/29/EC(「不公正な商慣行指令」)(OJ L 149, 11.6.2005,p.22)。

を与えるものであってはならない。さらに、広告の分野など、一般的かつ合法的な商慣行で、適用される法を遵守するものは、それ自体、AI を前提とする有害な操作行為を構成するとみなされない。

- (30) 個人の政治的意見、労働組合への加入、宗教上または思想上の信念、人種、性生活、または性的指向を推測または推論するために用いられる、顔や指紋などの自然人の生体データに基づく生体分類システムは禁止されなければならない。この禁止は、例えば法執行の分野において使用され得る髪の色や目の色による画像の選別など、生体データに基づき、EU 法または国内法に従って取得された生体データセットの合法的なラベリング、フィルタリング、または分類を対象とするものではない。
- (31) 公私の行為者による自然人のソーシャル・スコアリングを可能とする AI システムは、差別的な結果や一定のグループの排除をもたらし得る。それは、尊厳に対する権利および差別をうけない権利を侵害する可能性があり、かつ平等および正義の価値観に反する。これらの AI システムは、さまざまな文脈における社会的行動に関連する多様なデータポイントに基づいて、または一定期間における既知の、推論され、または予測される人の特徴または人格に基づいて、自然人または自然人のグループを評価しまたは分類する。当該 AI システムから得られるソーシャル・スコアは、データが当初生成または収集された文脈とは切り離された社会的文脈において、自然人またはそのグループ全体に対する有害または不利な取扱いを導き、またはその社会的行動の重大性に対して不均衡または不当に有害な取扱いを導く可能性がある。したがって、そのような容認できないスコアリング行為を前提とし、かつそのような有害または不利な結果を生じさせる AI システムは禁止されなければならない。この禁止は、EU 法および国内法に従って、ある特定の目的で実施される自然人の合法的な評価に影響を与えてはならない。

(32) 法の執行を目的とする、公衆がアクセス可能な場所内における自然人の「リアルタイム」遠隔生体認証のための AI システムの使用は、人口の大部分のプライバシーに影響を与え、絶え間ない監視の感覚を想起させ、集会の自由およびその他の基本的権利の行使を間接的に思いとどらせる可能性があることにより、関係者の権利および自由に特に介入する。自然人の遠隔生体認証を目的とする AI システムの技術的不正確性は、バイアスがかかった結果をもたらし、差別的な影響を引き起こす可能性がある。このバイアスがかかった結果や差別的な影響のリスクは、年齢、民族的属性、人種、性別、心身障害に関して、特に重大である。さらに、リアルタイムで運用されるシステムの使用は、影響が即時である事実および追加的検証または訂正を行う可能性が限られる事実により、法執行行為の文脈における関係者、またはそれによって影響を受ける関係者の権利および自由に対するリスクを増大させる。

(33) したがって、法の執行を目的としてこれらのシステムを使用することは、使用が実質的な一般の利益を達成するために必要最小限であり、その利益の重要性がリスクに勝る状況において、限定的に列挙され、かつ厳格に定義された状況を除き、禁止されなければならない。これらの状況は、次を対象とする。行方不明者を含む犯罪行為の被害者の捜索；自然人の生命または身体の安全に対する一定の脅威またはテロリスト攻撃の脅威；および本規則の附属書に列挙される刑事犯罪で、当該刑事犯罪が、関係する加盟国において、少なくとも 4 年間で最長期間とする自由刑または留置命令によって処罰され得るものであり、それが当該加盟国の法に定められている場合の犯罪者または被疑者の所在特定または身元特定。国内法に定める拘禁刑または留置命令についてのこのような基準値は、その犯罪が「リアルタイム」遠隔生体認証システムの使用を正当化するために十分に重大であることを保証することに寄与する。

さらに、本規則の附属書に定める刑事犯罪のリストは、欧州理事会枠組み決定 2002/584/JHA¹⁸ に列挙される 32 の刑事犯罪に基づくものであり、これらの犯罪のいくつかは、他の犯罪より実際に関連性が認められる事実を考慮するものであり、リアルタイム遠隔生体認証に頼ることは、害または潜在的悪影響の重大性、蓋然性または規模が異なり得ることもまた鑑み、列挙されたさまざまな刑事犯罪の一つの犯罪者または被疑者の所在特定または身元特定の実務的追跡手段として、非常にさまざまな段階において、おそらく必要かつ相応となり得る。また、自然人の生命または身体の安全に対する差し迫った脅威は、欧州議会および欧州理事会指令(EU)2022/2557¹⁹ 第 2 条(4)にいう重要インフラの深刻な混乱から生じ得るが、その場合、この重要インフラの停止または破壊は、特に、住民への基本的物資の供給または国家の本質的機能の実行に対する重大な侵害によって、人の生命または身体の安全に対する差し迫った脅威をもたらし得る。さらに、本

¹⁸ 2002 年 6 月 13 日の欧州の逮捕状と加盟国間の身柄引渡し手続きに関する理事会枠組み決定 2002/584/JHA(OJ L 190、2002 年 7 月 18 日、p.1)。

¹⁹ 重要な事業体のレジリエンスに関する、および理事会指令 2008/114/EC を廃止する 2022 年 12 月 14 日の欧州議会および欧州理事会指令 (EU) 2022/2557 (OJ L 333、27.12.2022、p. 164)。

規則は、法執行機関、出入国管理局、移民当局、または亡命を管轄する当局に、身元確認について、EU 法および国内法に定める条件に従って、関係者の立会いの下で身元確認を実施する権限を保持させるものでなければならない。特に、法執行機関、出入国管理局、移民当局、または亡命を管轄する当局は、本規則による事前の許可を得る義務を負うことなく、身元確認の際に、身元確認を拒否し、または身元を申告することもしくは証明することができない人を特定するため、EU 法または国内法に従って、情報システムを使用できなければならない。たとえば、犯罪の関係者で、事故またはその健康状態を理由に、法執行機関に対し、身元を明らかにすることを望まないか、明らかにすることができない場合である。

- (34) これらのシステムが確実に責任ある相応な方法で使用されるようにするため、限定的に列挙され、かつ厳格に定義された状況のそれぞれにおいて、特に、請求の原因となった状況の性質、およびすべての関係者の権利と自由に対する使用の結果、ならびに使用に関連するセーフガードと条件などに関し、考慮されるべき一定の要素を確立することもまた重要である。さらに、法の執行を目的とする、公衆がアクセス可能な場所内における「リアルタイム」の遠隔生体認証システムの使用は、具体的に対象となる人の身元の特定を確認するためにのみ行われるべきであり、かつ、使用は、特に脅威、被害者または犯罪者に関する証拠または通報に鑑み、期間、地理的および人的な範囲に関して、必要最小限なものに限定されなければならない。公衆がアクセス可能な場所内でのリアルタイム遠隔生体認証システムの使用は、管轄を有する法執行機関が、基本的権利に対する影響の分析を完了し、かつ、本規則に別段の定めがない限り、本規則に定めるデータベースにシステムを登録しない限り、認められるべきではない。人の参照データベースは、上記にいう各状況における各ユースケースに適合したものでなければならない。

(35) 法の執行を目的とする公衆がアクセス可能な場所内での「リアルタイム」遠隔生体認証認識システムのあらゆる使用は、司法当局または決定が拘束力を持つ加盟国の独立の行政当局による、明示的かつ特別な許可に基づくものでなければならない。この許可は、原則として、一人または複数の人を特定する目的で、AI システムの使用に先立ち、取得されなければならない。当該規定の例外は、緊急性を理由に十分に正当化される状況において、すなわち、問題となるシステムを使用する必要が、AI システムの使用を開始する前に許可を得ることを実質的かつ客観的に不可能とする状況において、認められなければならない。このような緊急の状況においては、AI システムの使用は、必要最小限に限定されなければならない。かつ、国内法において限定され、法執行機関自身により各緊急使用の文脈が特定されるような、適切なセーフガードおよび条件に従わなければならない。さらに、法執行機関は、そのような状況においては、不当に遅滞することなく、遅くとも 24 時間以内に、より早い段階で許可を請求できなかった理由を示しつつ、その許可を請求しなければならない。

許可の請求が拒絶された場合、この許可に関するリアルタイム生体認証システムの使用は直ちに停止され、かつ、この使用に関するすべてのデータは破棄および削除されなければならない。これらのデータには、このシステムの使用中に AI システムによって直接取得された入力データ、ならびにこの許可に関する使用の結果および出力が含まれる。他の国内法または EU 法に従って、合法的に取得された入力はこれに含まれない。いずれにせよ、人に対し不利な法的効果を生じさせるいかなる判断も、遠隔生体認証システムの出力のみに基づいて下されてはならない。

(36) 本規則および国内規定に定められた要件に従って任務を遂行するため、関係する市場監視当局および国内のデータ保護当局に対し、リアルタイム生体認証システムの各使用を通知しなければならない。通知を受けた市場監視当局および国内のデータ保護当局は、リアルタイム生体認証システムの使用に関する年次報告書を欧州委員会に提出しなければならない。

(37) さらに、本規則に定める網羅的な枠組みにおいて、本規則に従った加盟国領内における当該使用は、関係する加盟国がその国内法の詳細な規定において、当該使用を許可する可能性を明確に規定することを決定した場合にのみ、およびその範囲でのみ、可能であることを規定することが適切である。したがって、加盟国は、本規則に基づき、そのような可能性をまったく規定しないことも自由であり、または本規則に定める許可された使用を正当化できる目的のうち一定の目的についてのみ当該可能性を規定することも自由である。これらの国内規定は、その採択後 30 日以内に、欧州委員会に通知されなければならない。

- (38) 法の執行を目的とする公衆がアクセス可能な場所内での自然人のリアルタイム遠隔生体認証のための AI システムの使用は、必然的に、生体データの処理を通じて行われる。一定の例外を除き当該使用を禁止する、TFEU 第 16 条に基づく本規則のルールは、指令(EU)2016/680 第 10 条に定める生体データ処理に関するルールの遵守における特別法として適用され、そこでは、この使用、およびその結果である生体データの処理は限定的に規定される。したがって、当該使用および当該処理は、本規則により定められた枠組みと両立する範囲においてのみ可能とされなければならない。この枠組み外で法の執行を目的として管轄当局が行動する場合、指令(EU)2016/680 第 10 条に列挙される理由により、管轄当局がこれらのシステムを使用しかつ当該データを処理することは不可能である。この文脈において、本規則は、指令(EU)2016/680 第 8 条に基づく個人データの処理の法的基礎を提供することを目的とするものではない。しかし、管轄当局によるものを含め、法の執行以外の目的で公衆がアクセス可能な場所内においてリアルタイム遠隔生体認証システムを使用することは、本規則に定める法の執行を目的とする使用に関する特別な枠組みの対象とすべきではない。したがって、法の執行以外の目的での使用は、本規則およびこの許可に効力を与え得る適用される国内法の詳細なルールに基づく許可の要件の対象とすべきではない。
- (39) 本規則で規制される法の執行を目的とする公衆がアクセス可能な場所内でのリアルタイム遠隔生体認証システムを使用することに関係しない、生体認証のための AI システムの使用の際に用いられた生体データおよびその他の個人データのあらゆる処理は、指令(EU)2016/680 第 10 条に基づくすべての要件を引き続き遵守しなければならない。法の執行以外の目的については、規則(EU)2016/679 第 9 条第 1 項および規則(EU)2018/1725 第 10 条第 1 項は、これらの条項に定める限定的な例外は別として、生体データ処理を禁止する。規則(EU)2016/679 第 9 条第 1 項の適用により、法の執行以外の目的で遠隔生体認証を使用することは、既に各国のデータ保護当局により下される禁止決定の対象である。

- (40) TEU および TFEU に附属の、自由、安全および司法の領域に関する英国およびアイルランドの地位に関する議定書第 21 号第 6 条 a 条に従い、アイルランドが、TFEU 第 16 条に基づいて定められた規定の遵守を求める刑事分野の司法協力または警察協力の形式を規制するルールに拘束されない場合、アイルランドは、第 5 条第 1 項第 1 段落(g)に定めるルールについて、それが警察協力の分野および刑事司法協力の分野における活動のための生体分類システムの使用に適用される限りにおいて拘束されず、第 5 条第 1 項第 1 段落(d)に定めるルールについて、この規定の対象となる AI システムの使用に適用される限りにおいて拘束されず、本規則第 5 条第 1 項第 1 段落(h)、第 5 条第 2 項ないし第 6 項および第 26 条第 10 項に定めるルールで TFEU 第 3 部第 V 編第 4 章または第 5 章の適用対象となる活動の実行において構成国による個人データ処理に関し TFEU 第 16 条に基づいて採択されたルールについて、拘束されない。
- (41) TEU および TFEU に附属の、デンマークの地位に関する議定書第 22 号第 2 条および第 2a 条に従い、デンマークは、第 5 条第 1 項第 1 段落(g)に定めるルールについて、それが警察協力の分野および刑事司法協力の分野における活動のための生体分類システムの使用に適用される限りにおいて拘束されず、第 5 条第 1 項第 1 段落(d)に定めるルールについて、それがこの規定の対象となる AI システムの使用に適用される限りにおいて拘束されず、本規則第 5 条第 1 項第 1 段落(h)、第 5 条第 2 項ないし第 6 項および第 26 条第 10 項に定めるルールで TFEU 第 16 条に基づいて採択されたルールについて、それが TFEU 第 3 部第 V 編第 4 章または第 5 章の適用範囲となる活動の実行において構成国による個人データ処理に関する場合、拘束されず、それらの適用もされない。
- (42) 無罪の推定に従い、EU 域内の自然人は、常にその実際の行動に基づいて判断されなければならない。自然人は、その人が客観的に検証可能な事実に基づき犯罪行為に関与していると疑われる合理的な理由なく、かつ人による当該事実の評価なく、国籍、出生地、居住地、子どもの数、負債の程度、車の種類など、プロファイリング、その人格的特徴またはその特性のみを基礎として、AI によって予測される行動に基づき判断されてはならない。したがって、自然人のプロファイリングのみに基づき、またはその人格的特徴や特性の評価のみに基づき、その自然人が罪を犯す可能性を評価する目的で、または実際の犯罪もしくは潜在的な犯罪の発生を予測する目的で、自然人に関して実施されるリスク評価は、禁止されることが適切である。いずれにせよ、この禁止は、人のプロファイリングや個人の人格的特徴や特性に基づかないリスク分析を対象とするものではなく、関係もしない。たとえば、疑わしい取引に基づき企業が金融詐欺の可能性を評価するためのリスク分析に用いる AI システムや、既知の違法売買ルートなどに基づいて、税関当局による麻薬や違法な商品の所在特定の見込みを予測できるリスク分析ツールなどがこれにあたる。

- (43) インターネットまたは CCTV 映像から顔画像を無差別にスクレイピングすることにより、顔認識データベースを作成しまたは開発する AI システムを上市し、この特定の目的のためにサービスを開始し、または使用することは、大衆監視の感覚を強め、かつプライバシーの権利を含む、基本的権利への重大な侵害をもたらす得ることにより、禁止されなければならない。
- (44) 感情を識別しまたは推論することを目的とする AI システムの科学的根拠については、感情表現が文化や状況によって大きく異なり、同じ個人においてすら大きく異なるだけにいっそう深刻な懸念がある。当該システムの主要な欠点は、とりわけ、その限定的な信頼性、その正確性の欠如、およびその限定的な一般的適用可能性である。したがって、その生体データに基づき自然人の感情や意図を識別しまたは推測する AI システムは、差別的な結果をもたらす、かつ関係者の権利および自由を侵害する可能性がある。労働または教育の枠内において存在する力関係の不均衡を考える場合、これらのシステムの干渉的な性質と相俟って、これらのシステムは、一定の自然人または自然人のグループ全体に対し、有害または不利な取扱いをもたらすおそれがある。したがって、職場および教育に関する状況においては、自然人の感情の状態を検知するために使用されることを目的とする AI システムの上市、サービス開始、または使用を禁止することが適切である。この禁止は、治療用のシステムなど、厳密に医療上または安全上の理由により、上市される AI システムを対象とするものではない。
- (45) 本規則は、EU 法により禁止される行為、特に、データ保護法、差別禁止法、消費者保護法、競争法に基づき禁止される行為に、何ら影響しない。

(46) ハイリスク AI システムは、義務的な要件を充足している場合にのみ、EU 市場に上市され、サービスを開始され、または使用される。これらの要件は、EU 域内において利用可能なハイリスク AI システムまたは EU 域内においてほかに使用されるその出力が、EU 法により認められおよび保護される EU の重要な公共の利益に対し容認できないリスクを示さないよう、保証するものである。欧州委員会が、その通達である「EU 製品ルール 2022 の実施に関する『ブルーガイド』」²⁰において詳細を示した新たな立法枠組みに基づき、一般的ルールとして、欧州議会および欧州理事会規則(EU)2017/745²¹、規則(EU)2017/746²²、および欧州議会および欧州理事会指令 2006/42/EC²³などの EU 調和法の複数の法令が一製品に適用され得ることになるが、その製品は適用されるすべての EU 調和法を遵守している場合にのみ、利用に供されまたはサービスを開始できる。一貫性を確保するとともに、不要な管理上の負担やコストを避けるため、本規則および本規則の附属書記載のリストに記載される EU 調和法の要件が適用される 1 つ以上のハイリスク AI システムを含む製品の提供者は、1 つ以上の AI システムを含む製品が EU 調和法の適用されるすべての要件を最適な方法で遵守することを保証する方法に関する運用上の判断について、ある程度の柔軟性が必要である。ハイリスクであると指定される AI システムは、EU 域内の市民の健康、安全および基本的権利に対し非常に有害な影響を与えるシステムに限定されなければならない。かつ、そのような限定は国際貿易に対するあらゆる潜在的制限を最小限するものでなければならない。

(47) AI システムは、特に、このシステムが製品のセキュリティ・コンポーネントとして使用される場合、市民の健康および安全に悪影響を与え得る。EU 調和法の目的は域内市場における製品の自由な移動を促進すること、および安全でそのほかの点も適合した製品のみが上市されるよう保証することであるが、当該目的に従い、AI システムを含む、そのデジタル・コンポーネントにより製品全体に生じ得る安全上のリスクを、適切に防止しおよび軽減することが重要である。例えば、ますます自律型となるロボットは、製造の分野においてもまたは介護や介助の分野においても、複雑な環境において、安全に動作しかつその機能を発揮できるものでなければならない。同様に、生命および健康への関心が特に高い保健衛生分野においては、ますます高度となる診断システムおよび人間の診断を支援するシステムは、信頼性が高くかつ正確でなければならない。

²⁰ OJ C 247, 29.6.2022, p1.

²¹ 医療機器に関する 2017 年 4 月 5 日の欧州議会および理事会の規則(EU)2017/745、指令 2001/83/EC、規則(EC)No 178/2002 および規則(EC)No 1223/2009 を改正し、理事会指令 90/385/EEC および 93/42/EEC を廃止(OJ L 117, 5.5.2017, p.1)。

²² 体外診断用医療機器に関する 2017 年 4 月 5 日の欧州議会および理事会の規則(EU)2017/746、および指令 98/79 / EC および欧州委員会決定 2010/227 / EU の廃止(OJ L 117, 5.5.2017, p.176)。

²³ 機械に関する 2006 年 5 月 17 日の欧州議会および理事会の指令 2006/42 / EC、および指令 95/16 / EC の改正(OJ L 157, 9.6.2006, p.24)。

(48) 憲章により保護される基本的権利に AI システムが与える悪影響の規模は、AI システムをハイリスクとして分類する場合に、特に関連のある基準となる。これらの権利には、人間の尊厳に対する権利、私生活および家族生活の尊重、個人データの保護、表現および情報の自由、集会および結社の自由、差別をうけない権利、教育を受ける権利、消費者保護、労働者の権利、心身障害者の権利、ジェンダーの平等、知的財産権、効果的な救済と公正な裁判を受ける権利、弁護権と無罪の推定、および良好な行政に対する権利を含む。これらの権利に加え、次の事実を強調することが重要である。それは、子どもは、憲章第 24 条、およびデジタル環境に関する UNCRC のジェネラル・コメント第 25 号においてさらに進展した国連子どもの権利条約に記される特別な権利を享受しているとの事実、ならびにこれらのいずれもが、子どもの脆弱性を考慮することを求め、および子どもの福祉のために必要となる適切な保護と監護を提供することを求めるものであるとの事実である。憲章に記されかつ EU の政策で実施されるハイレベルな環境保護に対する基本的権利も、特に、人の健康と安全に関するものを含め、AI システムが生じさせ得る害の重大性を評価する際に考慮されなければならない。

- (49) 欧州議会および欧州理事会規則(EC)No 300/2008²⁴、欧州議会および欧州理事会規則(EU)No 167/2013²⁵、欧州議会および欧州理事会規則(EU)No 168/2013²⁶、欧州議会および欧州理事会指令 2014/90 / EU²⁷、欧州議会および欧州理事会指令(EU)2016/797²⁸、欧州議会および欧州理事会規則(EU)2018/858²⁹、欧州議会および欧州理事会の規則(EU)2018/1139³⁰ または欧州議会および欧州理事会規則(EU)2019/2144³¹の適用範囲となる製品またはシステムのセキュリティ・コンポーネントを構成するハイリスク AI システム、またはそれ自体がこれらの適用範囲となる製品またはシステムであるハイリスク AI システムに関し、これらの法に基づき関連する委任法令または実施法令を採択する際、各分野の技術的特性および規制上の特性に基づき、かつ、これらの規則に基づき既に導入されているガバナンス、適合性評価、施行のメカニズムおよび権限を妨げることなく、欧州委員会が、本規則に定めるハイリスク AI システムに適用される義務的な要件を考慮することを確保するため、これらの法を改正することが適切である。
- (50) 本規則の附属書に記載されている一定の EU 調和法の対象となる製品のセキュリティ・コンポーネントを構成する AI システム、またはそれ自体が当該製品である AI システムに関しては、関係の製品が対応する EU 調和法に従って第三者適合性評価機関により適合性評価手続きの対象となる場合、本規則に基づきそれらをハイリスクとして分類することが適切である。これらの製品とは、特に、機械、玩具、エレベーター、爆発可能性のある環境での使用を目的とする機器および保護システム、無線機器、圧力機器、レジャー用船舶機器、索道設備、ガス燃料を燃焼する機器、医療機器、体外診断用医療機器、車両および航空機である。
- (51) 本規則に基づく AI システムをハイリスクとして分類することは、セキュリティ・コンポーネントとして AI システムを用いる製品、または AI システム自体が製品であるものが、問題の製品に適用される対応する EU 調和法に定める基準に従ってハイリスクとみなされることを、必ずしも意味しない。これは、特に、規則(EU)2017/745 および(EU)2017/746 の場合であり、そこでは第三者による適合性評価は中程度のリスクおよびハイリスクの製品に対し定められる。
- (52) スタンドアロンの AI システム、すなわち、製品のセキュリティ・コンポーネントを構成するものまたはそれ自体が製品であるもの以外のハイリスク AI システムについては、その意図的に照らし、生じうる害の重大性およびその発生の可能性の双方を考慮し、人の健康、安全または基本的権利に害を生じさせる高度のリスクを示す場合、および本規則に定める相当数の特別に予め定義された分野において使用される場合、それらをハイリスクとして分類することが適切である。これらのシステムは、ハイリスク AI システムのリストの将来的なあらゆる修正のために想定される方法および基準と同じ方法および基準に基づき定義されるものであり、技術革新の急速なペースおよび AI システムの使用における変化の可能性を考慮するため、欧州委員会が、委任法令により、採択する権限を与えられるべきである。

²⁴ 民間航空のセキュリティ分野における共通ルールの導入に関する、および規則(EC)No 2320/2002

-
- を廃止する 2008 年 3 月 11 日の欧州議会および欧州理事会規則(EC)No 300/2008 (OJ L 97,9. 4. 2008, p.72)。
- 25 農林業車両の承認および市場監視に関する 2013 年 2 月 5 日の欧州議会および欧州理事会規則 (EU)No 167/2013(OJ L 60, 2.3.2013, p.1)。
- 26 二輪車または三輪車および四輪車の承認および市場監視に関する 2013 年 1 月 15 日の欧州議会および欧州理事会規則(EU)No 168/2013(OJ L 60, 2.3.2013, p.52)。
- 27 船舶用機器に関する、および理事会指令 96/98/EC の廃止する 2014 年 7 月 23 日の欧州議会および欧州理事会指令 2014/90/EU(OJ L 257, 28.8.2014, p.146)。
- 28 EU 内の鉄道システムの相互運用性に関する 2016 年 5 月 11 日の欧州議会および欧州理事会指令 (EU)2016/797(OJ L 138, 26.5.2016, p.44)。
- 29 自動車およびその牽引車、ならびにこれらの車両のためのシステム、コンポーネント、および単体技術ユニットの承認および市場監視に関する、ならびに規則(EC)No 715/2007 および(EC)No 595/2009 を改正し、指令 2007/46/EC を廃止する 2018 年 5 月 30 日の欧州議会および欧州理事会規則(EU)2018/858 (OJ L 151, 14.6.2018, p.1)。
- 30 民間航空分野における共通ルールに関するおよび EU 航空安全庁を設置する、ならびに欧州議会および欧州理事会規則(EC)No 2111/2005、(EC)No 1008/2008、(EU)No 996/2010、(EU)No 376/2014、および欧州議会および欧州理事会指令 2014/30/EU、2014/53/EU を改正し、欧州議会および欧州理事会規則 (EC) No52/2004、(EC) No216/2008、欧州理事会規則(EEC)No 3922/91 を廃止する、2018 年 7 月 4 日の欧州議会および欧州理事会規則(EU)2018/1139 (OJ L 212, 22.8.2018, p. 1)。
- 31 自動車およびその牽引車、ならびに当該車両のためのシステム、コンポーネント、および単体技術ユニットの型式承認要件に関する、一般的な安全性ならびに車両の乗員および交通弱者の保護について、欧州議会および欧州理事会規則(EU)2018/858 を改正し、および欧州議会および欧州理事会規則(EC)No 78/2009、(EC)No 79/2009 および(EC)No 661/2009、欧州委員会規則(EC) No 631/2009、(EU) No 406/2010、(EU) No 672/2010、(EU) No 1003/2010、(EU) No 1005/2010、(EU) No 1008/2010、(EU) No 1009/2010、(EU) No 19/2011、(EU) No 109/2011、(EU) No 458/2011、(EU) No 65/2012、(EU) No 130/2012、(EU) No 347/2012、(EU)No 351/2012、(EU)No 1230/2012、および(EU)2015/166 を廃止する 2019 年 11 月 27 日の欧州議会および欧州理事会規則(EU)2019/2144 (OJ L 325, 16.12.2019, p.1)。

(53) 本規則に定める予め定義された特定の分野において対象となる AI システムは、意思決定に実質的な影響を与えないか、またはこれらの利益に対し重大な害を生じさせないとの理由により、これらの領域において保護される法的利益を侵害する重大なリスクを示さない、特別の場合があり得ることを明確にすることもまた重要である。本規則の適用上、意思決定の結果に実質的な影響を与えない AI システムは、その決定が人間によるものか自動化されたものかを問わず、意思決定の内容に、したがって意思決定の結果に影響を与えない AI システムであると理解することが適切である。以下の 1 つ以上の条件が満たされる場合、意思決定の結果に実質的な影響を与えない AI システムといい得る。これらの条件の第 1 は、非構造化データを構造化データに変換すること、入力されたドキュメントをカテゴリに分類すること、または多数のアプリケーションの中から重複を検出することなど、AI システムが手続き上の狭いタスクを実行することを目的とすることである。これらのタスクは、あまりに狭くかつ限定的な性質のものであるため、本規則の附属書におけるハイリスクな使用として列挙されている文脈において、AI システムの使用により助長されない限定的なリスクしかない。第 2 の条件は、AI システムによって実行されるタスクが、以前に行われた人間の活動の結果を改善することを目的とすることであり、これは本規則の附属書に列挙されるハイリスクな使用目的に利用され得る。これらの特性を考慮すれば、AI システムは人間活動に補足的な層を追加するにすぎず、結果として、低減されたリスクを示すことになる。この条件は、例えば、プロフェッショナルな口調、アカデミックな言語スタイル、または一定のブランドメッセージに適合したテキストなど、既に起案された文書のスタイルを改善することを目的とした AI システムに適用されると考えられる。

第 3 の条件は、AI システムが意思決定パターンを検知し、または以前の意思決定パターンからの逸脱を検知することを目的とすることである。この AI システムの使用は、人間による評価実施の後にあり、かつ、人間による適切な検証なく、評価を置き換えることも、それに影響を与えることも目的としていないという理由により、リスクは低いと考えられる。例えば、採点において教師の一定の採点パターンを考慮し、教師がこれらの採点パターンから逸脱した可能性があるかどうかを事後的に検証するために、潜在的な不整合や異常にフラグを立てる方法により使用され得る AI システムがこれにあたる。第 4 の条件は、AI システムが、本規則の附属書に記載される AI システムの目的に関する評価の準備に過ぎないタスクを実行することを目的とし、したがって、システムの出力が事後的な評価にリスクを示す可能性が極めて低いことである。この条件は、とりわけ、インデックス化、検索、テキスト処理およびスピーチ処理、もしくは他のデータソースへのデータのリンクのような、さまざまな機能を含むファイル処理のためのスマートソリューション、または原文書の翻訳に使用される AI システムに適用される。いずれにせよ、本規則の附属書に列挙されるハイリスクなユースケースにおいて使用される AI システムは、AI システムが規則(EU)2016/679 第 4 条(4)、指令(EU)2016/680 第 3 条(4)および規則(EU)2018/1725 第 3 条(5)にいうプロファイリングを前提とする場合、健康、安全、または基本的権利に対して害を及ぼす重大なリスクを示すと見なされるべきである。トレーサビリティと透明性を保証するため、上記の条件に基づき AI システムがハイリスクではないと考える提供者は、このシステムが上市

されまたはサービスが開始される前に、評価文書を作成し、かつ請求に従ってこの文書を各国の所轄当局に提出しなければならない。この提供者は、本規則に基づき創設される EU データベースに、AI システムを登録する義務を負う。本規則の附属書に列挙される AI システムが、例外的にハイリスクなシステムではないとする条件の実務的な実施のため、追加的なガイダンスを提供する目的で、欧州委員会は、AI 委員会への諮問後、ハイリスク AI システムのユースケースおよびそうでない AI システムのユースケースの実例を限定列挙するリストを添付し、この実務的な実施を明記したガイドラインを提供しなければならない。

- (54) 生体データは個人データの特別な範疇を構成するものであるため、適用される EU 法および国内法がその使用を許可する範囲で、生体認証システムの重要ないくつかのユースケースを、ハイリスクとして分類することが適切である。自然人の遠隔生体認証を目的とする AI システムの技術的不正確性は、バイアスのかかった結果をもたらし得るものであり、かつ差別的な効果を引き起こし得る。このようなバイアスのかかった結果や差別的な効果のリスクは、年齢、民族的属性、人種、性別、心身障害に関して特に重要である。したがって、遠隔生体認証システムは、それらが呈するリスクを考慮し、ハイリスクとして分類することが適切である。特定の自然人がそれと主張する本人であると確認することを唯一の目的とする、およびサービスへのアクセス、デバイスのロック解除、または施設への安全なアクセスのみを目的として、自然人の同一性を確認することを唯一の目的とする、認証を含む、生体 1 対 1 認証の目的で使用されることを目的とする AI システムは、この分類から除外される。さらに、生体データの基礎となる規則(EU)2016/679 第 9 条第 1 項に基づき保護される機微な属性または特性に従って、生体分類のため使用されることを目的とする AI システムは、本規則により禁止されない限りハイリスクとして分類すること、および本規則により禁止されない感情認識システムはハイリスクとして分類することが適切である。サイバーセキュリティおよび個人データ保護措置を可能にする目的でのみ使用されることを目的とする生体認証システムは、ハイリスク AI システムと見なされるべきではない。
- (55) 重要インフラの管理および運用に関しては、指令(EU)2022/2557 附属書 I (8)に定める重要なデジタル・インフラの管理および運用、道路交通、水、ガス、電気および暖房の管理および運用の枠内におけるセキュリティ・コンポーネントとして使用されることを目的とする AI システムを、ハイリスクとして分類することが適切である。それらの障害または誤作動は、大々的に人の生命と健康を危険にさらし、社会的および経済的活動の通常の実行に重大な混乱を引き起こし得るからである。重要なデジタル・インフラを含む、重要インフラのセキュリティ・コンポーネントは、重要インフラの物理的完全性を直接的に保護するため、または人や財産の健康および安全を直接的に保護するために使用されるシステムであるが、システムの動作には必要ではない。これらのコンポーネントの障害または誤作動は、重要インフラの物理的完全性に対するリスク、ひいては人や財産の健康および安全に対するリスクを、直接的に引き起こし得る。サイバーセキュリティの目的のみに使用されることを目的とするコンポーネントは、セキュリティ・コンポーネントとみなされるべきではない。これら重要インフラのセキュリティ・コンポーネントの例として、水圧を監視するシステムや、クラウド情報処理センター内の火災警報制御システムがある。

(56) 教育における AI システムの導入は、質の高いデジタル教育および職業訓練を促進するため、および経済、社会および民主的プロセスに積極的に参加するために、すべての学習者および教員が、メディアリテラシー、批判的精神を含む、必要なデジタルスキルおよび能力を習得しかつ共有できるようにするために、重要である。ただし、特に、あらゆるレベルの教育および職業訓練の機関またはプログラムに対するアクセスまたは入学許可の決定のため、それらに対する所属の決定のため、人の習得の成果の評価するため、その人が享受するまたはアクセスできる教育および職業訓練のレベルに重大な影響を与える人の適切な教育レベルを評価するため、または試験中に学生を監視するためおよびその枠内において禁止行為を探知するために、教育または職業訓練において使用される AI システムは、ハイリスク AI システムとして分類されなければならない。それは、それらの AI システムが、人の教育コースおよび専門コースを決定する可能性があり、したがって、自身の生計を確保する人の能力に対して影響を与える可能性があるからである。それらが不適切に設計され使用される場合、これらのシステムは、特に干渉的となり得、教育および職業訓練を受ける権利、ならびに差別されない権利の侵害をもたらす可能性があり、例えば、女性、一定の年齢のグループ、心身障害者、またはその人種的もしくは民族的出自またはその性的指向を理由とする一定の人に対し、過去に由来する差別のパターンを永続させる可能性がある。

(57) 雇用、労働者管理および自営業へのアクセスに関する問題のために使用される AI システム、特に、人の採用および選考、労働関係の条件および労働上の契約関係における昇進および解除に影響を与える意思決定、個人の行動、人の個別的特徴または特性に基づく業務の割り当てのため、および労働上の契約関係の枠内における人の監視または評価のために使用される AI システムもまた、ハイリスクとして分類されなければならない。それは、これらのシステムが、将来のキャリアの見通し、これらの人の生計の手段、および労働者の権利に対して、重大な影響を与え得るからである。問題の労働上の契約関係はまた、2021 年欧州委員会労働プログラムに定めるように、有意な方法で、プラットフォーム上でサービスを提供する従業員および人がそれに関与しなければならぬ。採用プロセス全体において、および労働上の契約関係における人の評価、昇進、または雇用継続の際、AI システムは、例えば、女性、一定の年齢のグループ、心身障害者またはその人種的もしくは民族的出自またはその性的指向を理由とする一定の人に対し、過去に由来する差別のパターンを永続させる可能性がある。これらの人のパフォーマンスおよび行動を監視するために使用される AI システムは、データ保護およびプライバシーに対するそれらの基本的権利を侵害する可能性もある。

(58) AI システムの利用が特別な考慮に値するもう一つの分野は、人々が社会に完全に参加することを可能とし、または生活水準を向上させることを可能とするため必要な、一定の不可欠な、民間および公共のサービスならびに給付へのアクセスおよび権利である。特に、医療サービス、社会保障給付、出産・病気・労働災害・扶養・高齢・失業・社会扶助、・住宅手当などの場合において保護を提供する社会サービスなど、公権力の一部である不可欠な公的扶助の給付およびサービスを申請または受給している自然人は、あまねく、これらの給付やサービスに依存し、管轄当局との関係において脆弱な立場にある。受益者が給付およびサービスを受ける権利を合法的に有しているかどうかを判断することを含む、これらの給付およびサービスが当局によって付与され、拒否され、削減され、取消され、または返却されるべきかどうかを判断するために、AI システムが使用される場合、AI システムは、人々の生計の手段に大きな影響を与える可能性があり、かつ、社会的保護を受ける権利、差別をうけない権利、人間の尊厳に対する権利、効果的な救済を受ける権利などの人々の基本的権利を侵害する可能性があり、したがって、ハイリスクとして分類されなければならない。しかし、本規則は、これらのシステムが自然人および法人に対し高度なリスクを引き起こさないことを条件として、適合性のある安全な AI システムのより広範な使用から利益を得るであろう、行政における革新的なアプローチの開発および使用を妨げるべきではない。

さらに、自然人の信用スコアまたは支払能力を評価するために使用される AI システムは、これらの人々の財源へのアクセス、または住宅・電気・電気通信サービスなどの不可欠なサービスへのアクセスを決定するものであるから、ハイリスク AI システムとして分類されなければならない。これらの目的で使用される AI システムは、個人間またはグループ間の差別をもたらす可能性があり、かつ、人種的または民族的出自、性別、心身障害、年齢、性的指向に基づく差別などの、過去に由来する差別のパターンを永続させる可能性があり、または新しい形態の差別的影響を生む可能性がある。しかし、金融サービスの提供における詐欺を探知するため、ならびに金融機関および保険会社の自己資金の必要を計算するための諮問のために、EU 法に定める AI システムは、本規則においてハイリスクと見なされるべきではない。加えて、健康保険や生命保険の分野で、自然人に関するリスク評価および保険料の決定のために使用されることを目的とする AI システムは、これらの人々の生計の手段に大きな影響を与える可能性があり、それが適切に設計され、開発されおよび使用されない場合、基本的権利を侵害する可能性があり、金融排除および差別を含む、人々の生命および健康に対し重大な結果を引き起こす可能性がある。最後に、自然人による緊急通報を評価しかつ分類するために使用される AI システム、または、警察、消防および医療救援、ならびに救急医療サービスにおいて認められる患者のトリアージシステムなどの緊急初動対応サービスにおける、サービス派遣または優先順位の確立のために使用される AI システムも、人々の生命、健康および財産に対し、非常に重要な状況における判断を下すことになるため、ハイリスクに分類されなければならない。

(59) 法執行機関の役割と責任を考慮すると、AI システムの一定の使用を前提として法執行機関により行われる行為は、相当程度の力の不均衡を特徴とし、かつ、自然人の自由の監視、逮捕または剥奪、および憲章により保証される基本的権利に対するその他の悪影響をもたらし得る。特に、AI システムが高品質のデータで訓練されていない場合、そのパフォーマンス、精度または堅牢性に関して必要な要件を充足していない場合、または適切に設計されずかつ上市前もしくはサービス開始前にテストされていない場合には、差別的な方法、またはより一般的には、不適切もしくは不当な方法で、人々を取扱う危険がある。さらに、効果的な救済をうける権利および公正な裁判を受ける権利、ならびに弁護権および無罪の推定など、重要な手続上の基本的権利の行使は、特に、これらの AI システムが、十分な透明性がなく、説明可能でなくかつ文書化されていない場合に、妨げられる可能性がある。したがって、悪影響を回避し、公衆の信頼を維持し、かつ説明責任および効果的な救済を保証するため、精度、信頼性および透明性が特に重要である法執行の文脈において使用されることを目的とする多くの AI システムは、適用される EU 法および国内法がその使用を許可する範囲で、ハイリスクとして分類することが適切である。

活動の性質およびそれに関するリスクを考慮して、これらのハイリスク AI システムは、特に、ある自然人が刑事犯罪の被害者になるリスクを法執行機関が評価することを支援するため、ポリグラフおよび同様のツールとして法執行機関を支援するため、刑事犯罪の捜査または訴追の過程で証拠の信用性を法執行機関が評価することを支援するため、および本規則が禁止しない限りで、自然人のプロファイリングのみに基づくのではなく、自然人またはそのグループの個別的特徴、特性または前科前歴に基づき、自然人の犯罪行為のリスクまたは再犯のリスクを法執行機関が評価することを支援するため、刑事犯罪の探知、捜査および刑事訴追の枠内で、プロファイリングの目的で法執行機関を支援するため、法執行機関によってもしくはその名で、または EU の機関、組織、部署または事務所によって、使用されることを目的とする AI システムを含むものでなければならない。税務署および税関が行政手続きのために使用すること、およびマネーロンダリング防止に関する EU 法の枠内において、情報を分析する行政上の任務を遂行する金融情報機関が特に行政手続きのため使用することを目的とする AI システムは、刑事犯罪の防止および探知、捜査、刑事訴追の目的で、法執行機関によって使用されるハイリスク AI システムとして分類されるべきではない。法執行機関またはその他の関係当局による AI ツールの使用は、不平等または排除の要因となってはならない。特にこれらのツールの機能に関する有用な情報を得ることの困難さ、その結果、特に捜査中の自然人が法廷においてその結果に異議を述べることの困難さは、被疑者の弁護権に関する AI ツールの使用の影響として、無視されるべきではない。

(60) 移民、亡命および出入国管理の分野において用いられる AI システムは、しばしば特に脆弱な立場にある者、および、管轄の公的機関の行為の結果から逃れられない者に影響を与える。したがって、これらの文脈において使用される AI システムの精度、非差別性、透明性は、特に、移動な自由に対する権利、差別を受けない権利、プライバシーの保護および個人データの保護に対する権利、国際的な保護に対する権利、ならびに良好な行政に対する権利といった、関係者の基本的権利に対する尊重を保証するために、特に重要である。したがって、適用される EU 法および国内法がその使用を許可する範囲において、たとえば、ポリグラフおよび同様のツールとして、加盟国の領土に入国する自然人またはビザもしくは亡命を申請する自然人によって示される一定のリスクを評価するため、証拠の信用性に関する評価を含む、移民、亡命および滞在許可の申請の審査および許可を申請する自然人の適格性を定める目的に関して関係する不服の審査を実施することについて管轄の公的機関を支援するため、ならびに渡航書類の確認を除く、移民、亡命および出入国管理の枠内において、自然人を探知し、認識または識別する目的で、移民、亡命および出入国管理の分野において、管轄の公的機関によってもしくはそれらに代わり、または任務を負う EU の機関、組織、部署または事務所によって、使用されることを目的とする AI システムは、ハイリスクとして分類することが適切である。

本規則の対象となる移民、亡命、出入国管理の分野において使用される AI システムは、欧州議会および欧州理事会規則(EC)No 810/2009³²、欧州議会および欧州理事会指令 2013/32/EU³³、ならびにその他の関係する EU 法に定める関係する手続要件に適合するものでなければならない。AI システムは、いかなる状況においても、移民、亡命、出入国管理の分野において、1951 年 7 月 28 日にジュネーブで締結され、1967 年 1 月 31 日の議定書によって修正された、難民の地位に関する国連条約に基づいて課せられる国際的義務を回避する手段として、加盟国または EU の機関、組織、部署または事務所によって、使用されてはならない。また、方法のいかんを問わず、ノン・ルフールマン原則を破るためにも、または国際的な保護を受ける権利を含む EU の域内への安全かつ効果的な法的アクセス手段を拒否するためにも、使用されてはならない。

³² ビザに関する共同体コード(ビザコード)を定める 2009 年 7 月 13 日の欧州議会および欧州理事会規則(EC)No 810/2009(OJ L 243, 15.9.2009, p.1)。

³³ 国際的保護の付与および撤回の共通手続に関する 2013 年 6 月 26 日の欧州議会および欧州理事会指令 2013/32/EU (OJ L 180, 29.6.2013, p.60)。

- (61) 司法および民主的プロセスの管理運営のために使用されることを目的とする一定の AI システムは、民主主義、法の支配、個人の自由、ならびに効果的な救済を受ける権利および公正な裁判を受ける権利に対し、その重大な潜在的影響を考慮し、ハイリスクとして分類されなければならない。特に、バイアス、過誤および不透明性のリスクに対処するため、司法当局が事実および法律を調査および解釈し、一連の具体的事実に法律を適用することを支援する司法当局または司法当局に代わって使用されることを目的とする AI システムは、ハイリスク AI システムとして分類されることが適切である。これらの目的で ADR 機関が使用することを目的とする AI システムは、同様に、ADR 手続きの結果が当事者に法的効果を生じさせる場合、ハイリスクであるとみなされなければならない。AI ツールの使用は、裁判官の意思決定権限または司法の独立性を支援し得るが、最終的な意思決定は人間の行為によるべきであるから、それに置き換わるものであってはならない。しかし、AI システムをハイリスクであると分類することは、司法判断、文書またはデータの匿名化もしくは仮名化、職員間のコミュニケーションまたは管理運営業務など、個別のケースにおける司法の実際の管理運営に何ら影響を与えない、純粋に付随的な管理運営活動を目的として使用されることを目的とする AI システムにまで及ぶものではない。
- (62) 欧州議会および欧州理事会規則 (EU) 2024/...³⁴に定めるルールを害することなく、かつ、憲章第 39 条に記される投票権に対する不当な外部干渉のリスク、ならびに民主主義および法の支配に対する悪影響のリスクに対処するため、選挙もしくは国民投票の結果に影響を与える、または選挙もしくは国民投票の際に、その選挙権の行使における自然人の投票行動に影響を与えるために使用されることを目的とする AI システムは、ハイリスク AI システムとして分類されなければならない。これには、管理運営上および支援体制上の観点から政治キャンペーンを組織し、最適化しおよび構成するために用いられるツールのような、その出力が直接的に自然人に影響しない AI システムを除く。

³⁴ 政治広告の透明性およびターゲティングに関する欧州議会および欧州理事会規則(EU)2024/..... (OJ L, ..., ELI: ...).

+ OJ:文書 PE 90/23(2021/0381(COD)) に示される規則の番号を本文に記入し、かつ対応する脚注を完成させてください。

(63) 本規則に基づき AI システムがハイリスクとして分類されている事実は、システムの使用が、特に個人データ保護、もしくはポリグラフおよび同様のツールの使用、または自然人の感情の状態を探知する他のシステムの使用などに関し、EU の他の法令に基づき、または EU 法と両立する国内法に基づき、合法であることを示すものと解釈されてはならない。この種のあらゆる使用は、憲章に基づく適用要件、ならびに EU 派生法および国内法の適用法令に基づく適用要件に引き続き従わなければならない。本規則に別段の明示の定めがない限り、本規則が、必要に応じ、特別な種類の個人データを含む、個人データの処理のための法的根拠を構成するものとみなすことはできない。

(64) 上市されまたはサービスが開始されるハイリスク AI システムに関するリスクを軽減するため、かつハイレベルな信頼性を保証するため、AI システムの意図目的およびその使用の文脈、および提供者が実施するリスク管理体制を考慮し、一定の義務的要件が、ハイリスク AI システムに適用されなければならない。本規則の義務的要件を遵守するため提供者が採用する措置は、AI に関し一般的に認められる最先端技術を考慮し、かつ本規則の目的を達成するために相応かつ効果的でなければならない。新たな立法枠組みを前提に、「製品に対する EU のルール実施に関する『ブルーガイド』2022」と題する欧州委員会の通達において明確にされているように、適用されるすべての EU 調和法を製品が遵守している場合にのみ、利用に供されまたはサービス開始がおこなわれるのであるから、問題となる 1 つの製品に対し、EU 調和法の複数の立法が適用され得ることが一般的なルールである。本規則の要件の対象となる AI システムの危険性は、既存の EU 調和法に表明される側面とは異なる側面に関係するため、本規則の要件は、既存の EU 調和法の全体を補完する。たとえば、AI システムを組み込んだ医療機械や医療装置は、この分野の立法が AI システムに特有のリスクを取扱っていないため、関連する EU 調和法に定める健康および安全に関する本質的要件の対象とされていないリスクを示す可能性がある。

これは、さまざまな法令の同時かつ補完的な適用を前提とする。一貫性を確保し、不要な管理上の負担および不要な費用を回避するため、本規則の要件および本規則の附属書記載のリストにある新たな立法枠組みに基づく EU 調和法の要件が適用される、1 つ以上のハイリスク AI システムを含む製品の提供者は、1 つ以上の AI システムを含む製品が、この EU 調和法の適用要件全体を最適な方法で遵守することをどのように保証するかに関し採用する運用上の判断について、一定の柔軟性を持たなければならない。この柔軟性とは、例えば、本規則に基づき必要とされるテストプロセスおよび申告プロセス、ならびに要求される情報および文書の一部を、新たな立法枠組みに基づきかつ本規則の附属書に列挙されている既存の EU 調和法に基づき要求される既存の文書や手続きに統合することを、提供者が判断することを意味し得る。これは、適用されるすべての要件を遵守するという提供者の義務をいかなる場合にも害するものではない。

(65) リスク管理体制は、ハイリスク AI システムのライフサイクル全般にわたって、計画されかつ実行される、継続的かつ反復的なプロセスにより構成されなければならない。このプロセスは、健康、安全および基本的権利に対して生じる AI システムに関係するリスクを特定しかつ軽減することを目的とするものでなければならない。リスク管理体制は、その継続的な有効性を保証するため、ならびに本規則に基づき下されたあらゆる重要な判断および取られた措置の正当性および文書化を保証するために、定期的に検証されかつアップデートされなければならない。このプロセスは、提供者がリスクまたは悪影響を特定することを保証し、および AI システムとその動作環境との間の相互作用から生じ得るリスクを含む、その意図目的および合理的に予見可能な誤用に照らし、健康、安全および基本的権利に対する AI システムの既知のリスクおよび合理的に予見可能なリスクの軽減措置を実施することを保証するものでなければならない。リスク管理体制は、AI 分野の最先端技術に照らし、最適なリスク管理措置を採用するものでなければならない。最適なリスク管理措置を定める場合、提供者は行った選択を文書化し、かつ説明し、必要に応じて専門家および外部のステークホルダーと連携しなければならない。ハイリスク AI システムの合理的に予見可能な誤用を特定する場合、AI システムの使用が意図目的により直接的に対象とされていないとしても、かつ使用説明書中に警告されていないとしても、提供者は、特定の AI システムの特徴および特定の使用の文脈において容易に予見可能な人の行動から生じる合理的に予見できる AI システムの使用を対象としなければならない。

健康、安全または基本的権利に対するリスクを引き起こし得る、意図目的に従った、または合理的に予見可能な誤用の条件下における、ハイリスク AI システムの使用に関連する既知のまたは予見可能なあらゆる状況は、提供者が提示する使用説明書に記載されなければならない。これは、導入者が、ハイリスク AI システムを使用する際、それを認識し、かつ考慮するように確保するためである。本規則に基づき予見可能な誤用の場合のリスク軽減措置を特定しかつ実施することは、予見可能な誤用を是正するための、提供者による、ハイリスク AI システムに対する特別な追加的な訓練を要求するものであってはならない。しかし、提供者は、合理的に予見可能な誤用を軽減するために、必要かつ適切な場合、そのような追加的な訓練の措置を検討することが推奨される。

(66) リスク管理、使用されるデータセットの品質および関連性、技術文書および記録保存、透明性および導入者に対する情報提供、人間による管理、ならびに堅牢性、精度および安全性に関し、ハイリスク AI システムに対して、要件が適用されなければならない。これらの要件は、健康、安全および基本的権利に対するリスクを効果的に軽減するために必要である。取引についてより制限的でない他の措置が合理的に利用可能でなければ、これらの要件は取引に対する不当な制限を構成しない。

(67) 高品質のデータおよびこれらのデータへのアクセスは、特に、モデルの訓練を前提とする技術が使用される場合、多くの AI システムの構造を提供しかつパフォーマンスを確保する上で、重要な役割を果たす。これは、ハイリスク AI システムが目的としたようにかつ安全に機能することを保証するため、および EU 法により禁止される差別の原因にならないように保証するためである。高品質の訓練用、検証用およびテスト用データセットには、適切なデータガバナンスおよびデータ管理の実務の実施が必要である。ラベルを含む、訓練用、検証用およびテスト用のデータセットは、関連性があること、十分に代表的であること、および可能な限りエラーがなく、システムの意図目的との関係で完全であることが必要である。規則(EU)2016/679 などのデータ保護に関する EU 法の遵守を促進するため、データガバナンスおよびデータ管理の実務は、個人データの場合、データ収集の当初の目的に関する透明性を含むものでなければならない。また、データセットは、適切な統計上の特性を有するものでなければならない。これには、特に、出力データが将来の操作のための入力に影響を与える場合(フィードバックループの場合)において、人の健康および安全を害し得るデータセット、および基本的権利に悪影響を及ぼし得るデータセット、または EU 法により禁止されている差別を引き起こし得るデータセットにおける、潜在的バイアスを軽減することに特別な注意を払い、ハイリスク AI システムが使用されることを目的とする人または人のグループに関するものを含む。バイアスは、たとえば、特に、履歴データが使用される場合、基礎となるデータセットに内在することがあり、または、システムがリアルワールドにおいて実行される場合に生成されることがある。

AI システムにより生じる結果は、それらの内在的バイアスにより影響を受ける可能性があり、特に、人種や民族グループを含む、一定の脆弱なグループに属する人々に対し、徐々に強められる傾向にあり、したがって、既存の差別を永続させ、かつ増幅させる傾向がある。データセットが可能な限り完全でありかつエラーがないという要件は、AI システムの開発およびテスト実施の文脈におけるプライバシー保護技術の使用に影響を与えるべきではない。特に、データセットは、その意図目的に必要な範囲で、AI システムが使用されることを目的とする特定の地理上、文脈上、行動上、または機能上の環境に特有の特徴、特性、または要素を考慮しなければならない。データガバナンスに関連する要件は、データに関する本規則の要件の遵守が保証される限り、データガバナンスの検証、データセットの完全性、データの訓練、検証、およびテスト実施の実務を含む、認証されたコンプライアンスサービスを提供する第三者に依頼することにより、遵守され得る。

- (68) ハイリスク AI システムの開発および評価のため、提供者、認証機関のような一定の行為者、および欧州デジタルイノベーションハブ、試験・実験施設ならびに研究センターのようなその他の関連団体は、本規則に関係するこれらの者の活動領域において、高品質のデータセットにアクセスし、かつ使用することができなければならない。欧州委員会が創設した欧州共通データスペース、および企業間および政府との公共の利益のデータ共有の促進は、AI システムの訓練、検証およびテスト実施のための高品質なデータに対する信頼性があり、説明可能で、かつ差別のないアクセスを提供するために、重要となる。例えば、健康の分野においては、欧州健康データスペースは、プライバシーを尊重し、安全で、迅速で、透明性がありかつ信頼できる方法で、適切な制度化されたガバナンスとともに、健康データへの非差別的なアクセスを促進し、およびこれらのデータセットによる AI のアルゴリズムの訓練を促進することになる。また、データへのアクセスを提供しまたは促進する部門当局を含む、関係の管轄当局は、AI システムの訓練、検証およびテスト実施のための高品質なデータ提供を支援することができる。
- (69) プライバシーの権利および個人データの保護に対する権利は、AI システムのライフサイクル全般にわたり保証されなければならない。この点に関して、データ保護に関する EU 法に定められるように、設計によるおよびデフォルトによる、データ最小化およびデータ保護の原則は、個人データが処理される場合に適用される。これらの原則の遵守を保証するため、提供者が講じる措置には、本規則に定めるデータガバナンスの要件を害することなく、当事者間の送信なくまたは生データまたは構造化データ自体のコピーなく、匿名化および暗号化だけでなく、アルゴリズムをデータに導入することを可能にし、および AI システムのトレーニングを可能にする技術の使用も含まれ得る。
- (70) AI システムにおけるバイアスから生じ得る差別から他者の権利を保護するため、提供者は、例外的に、およびハイリスク AI システムに関するバイアスの検出および訂正の目的で厳密に必要な範囲内において、自然人の基本的権利および自由のための適切なセーフガードを条件として、かつ規則(EU)2016/679 および(EU)2018/1725 ならびに指令(EU)2016/680 に定める条件に加え、本規則に定める適用されるすべての条件の適用した上で、規則(EU)2016/679 第 9 条第 2 項(g)および規則(EU)2018/1725 第 10 条第 2 項(g)という重要な公共の利益を理由とする、特別な種類の個人データも処理できなければならない。

- (71) ハイリスク AI システムのトレーサビリティを可能にするため、本規則の要件の遵守を検証するため、ならびに問題のシステムの動作を監視しおよび市販後モニタリングを確保するため、ハイリスク AI システムがどのように開発され、そのライフサイクル全般にわたりどのように動作するかについて、理解可能な情報を保存することが不可欠である。これには、AI システムが関連する要件に適合しているかどうかを評価するために、およびその市販後モニタリングを容易にするために必要とされる情報を含む、技術文書の記録保存および利用可能性を必要とする。これらの情報には、特に、システムの一般的な特性、性能および限界が含まれ、アルゴリズム、データおよび訓練・テスト・検証プロセスが含まれ、ならびに明確かつ網羅的な形式で実施されかつ策定されるリスク管理体制に関する情報が含まなければならない。技術文書は、AI システムのライフサイクル全般にわたり、十分にアップデートされた状態に保たなければならない。さらに、ハイリスク AI システムは、技術面において、そのシステムのライフサイクル全般にわたり、ログを用い、イベントを自動的に記録できるものでなければならない。
- (72) 一定の AI システムの不透明性および複雑性に関する懸念に対処するため、かつ導入者が本規則に基づき課せられる義務を履行することを支援するため、ハイリスク AI システムについて、その上市前またはサービス開始前に、透明性が要求されなければならない。ハイリスク AI システムは、導入者が、AI システムの動作を理解し、その機能を評価し、かつ能力および限界を理解できるように設計されなければならない。ハイリスク AI システムは、使用説明書の形式で、適切な情報を伴わなければならない。これらの情報は、AI システムの特性、パフォーマンス、および性能の限界を含むものでなければならない。これらには、AI システムが健康、安全および基本的権利に対するリスクを引き起こし得る状況における、システムの動作およびパフォーマンスに影響を与え得る導入者の行為を含む、ハイリスク AI システムの使用に関する既知のおよび予見可能な潜在的状況に関する情報、提供者により適合性のために事前に決定されかつ評価されていた変更に関する情報、ならびに、導入者による AI システムの出力の解釈を容易にするための措置を含む、関係する人間による管理措置に関する情報が該当し得る。透明性は、システムに付属する使用説明書を含めて、導入者がシステムを使用すること、および事情を知った上で判断を下すことを支援するものでなければならない。導入者は、とりわけ、導入者に適用される義務に照らし、使用を意図するシステムについて正しい選択を行うためのより良い立場にあること、予定される使用および禁止される使用について情報を与えられること、必要に応じ AI システムを正しく使用することが必要である。使用説明書に記載される情報の読みやすさおよびアクセス可能性を高めるため、必要に応じ、たとえば、AI システムの制限について、および予定される使用と禁止される使用について、図表入りの例示を含めることが適切である。提供者は、使用説明書を含むすべてのドキュメントが、ターゲットである導入者のニーズおよび予見可能な知識を考慮し、有用で、完全で、アクセス可能で、かつ理解可能な情報を含むものであることを確保しなければならない。使用説明書は、関係する加盟国が決定する、ターゲットである導入者が容易に理解できる言語で利用できるものでなければならない。

- (73) ハイリスク AI システムは、意図されたとおりに使用されることを確保し、およびその影響がそのライフサイクル全般にわたり考慮されることを確保する方法で、ならびに自然人がその動作を管理し得る方法で、設計および開発されなければならない。そのために、システムの提供者が、システムの上市前またはサービス開始前に、適切な人間による管理措置を導入しなければならない。そのような措置は、必要に応じ、特に、システムがそれ自体によってオーバーライドされ得ない組み込まれた運用上の制約のもとに置かれること、システムが人間のオペレータの命令に応答すること、人間による管理を委ねられた自然人がその役割を果たすために必要な能力を有し、訓練を受け、および権限を有していることを、確保するものでなければならない。また、必要に応じ、ハイリスク AI システムは、人間による管理を委ねられた自然人が、悪影響やリスクを回避するため、または想定したように機能しないシステムを停止するために、介入するかどうか、いつ、どのように介入するかについて、情報に基づいた判断ができるよう、誘導しおよび通知することを目的とするメカニズムが含まれていることを確保することが不可欠である。特定の生体認証システムによって行われる不正確な一致の場合における人への重大な結果を考慮すると、少なくとも2名の自然人により、別々に、特定事項の検証および確認がされない限り、システムにより得られる特定事項に基づき、導入者がいかなる措置も判断も行うことができないような方法で、当該システムについて、人数を増やした人間による管理の要件を定めることが適切である。これらの者は1つ以上の団体に所属し得、システムを運用させまたは使用させる者を含み得る。この要件は、不要な負担または遅滞を生じさせるものであってはならず、異なる者が別々に実施する検証が、システムによって生成されたログに自動的に記録されることで十分である。法執行行為、移民、出入国管理、亡命の分野の特殊性を考慮すると、EU 法または国内法がその要件の適用が不相応であると判断する場合には、この要件は適用されるべきではない。
- (74) ハイリスク AI システムは、そのライフサイクル全般にわたり、絶えず機能し続けなければならない、ならびにその意図目的に照らし、および一般的に認められる最先端技術に従って、適切なレベルの精度、堅牢性、およびサイバーセキュリティを確保しなければならない。欧州委員会、ならびに関係する団体およびステークホルダーは、AI システムのリスクの軽減および悪影響を十分に考慮することが推奨される。期待されるレベルのパフォーマンス・メトリクスは、システムに添付される使用説明書に示されなければならない。提供者は、誤解のないまたは誤解させる表明のない、明確かつ理解しやすい方法で、導入者に対し、当該情報を伝達することが強く求められる。欧州議会および欧州理事会指令 2014/31/EU³⁵および指令 2014/32/EU³⁶を含む、法定計量に関する EU 法は、計測の精度を保証すること、および商取引の透明性と誠実性に貢献することを目的とする。この文脈において、欧州委員会は、計量当局やベンチマーク当局などの関係するステークホルダーおよび団体と協力し、必要に応じ、AI システムのベンチマークおよび測定方法の開発を奨励しなければならない。そうすることによって、欧州委員会は、AI に関して、計量法および関連する測定指標について作業する国際的パートナーに配慮し、かつそれらと協力しなければならない。

³⁵ 非自動重量計の上市に関する加盟国の法律の調和に関する 2014 年 2 月 26 日欧州議会および欧州理事会指令 2014/31/EU (OJ L 96, 29.3.2014, p.107)。

³⁶ 計量器の上市に関する加盟国の法律の調和に関する 2014 年 2 月 26 日の欧州議会および欧州理事会指令 2014/32/EU (OJ L 096, 29.3.2014, p.149)。

- (75) 技術的な堅牢性は、ハイリスク AI システムの重要な要件である。システム内の、またはシステムの動作環境内の限界に起因し得る、有害な、またはより一般的には、望ましくない動作（たとえば、エラー、障害、不整合および予期しない状況）に対して、レジリエンスがなければならない。したがって、ハイリスク AI システムの堅牢性を確保するため、たとえば、有害な、またはより一般的には、望ましくない動作を防止し、または最小限に抑えるため、適切な技術的ソリューションを設計しおよび開発することによる、技術的および組織的な対策が講じられなければならない。これらの技術的ソリューションには、なんらかの異常が存在する場合、または動作が事前に定められた一定の制限外で行われた場合に、たとえば、システムがその動作を安全に中断できるメカニズム（フェイルセーフプラン）を含み得る。これらのリスクに対する保護がなければ、たとえば、誤った判断または AI システムによって生成された誤った出力もしくはバイアスがかった出力により、安全に対する影響が生じ得、または基本的権利に対する悪影響を引き起こし得る。
- (76) サイバーセキュリティは、システムの脆弱性を利用する悪意のある第三者による AI システムの使用・動作もしくはパフォーマンスを変更する試み、またはそのセキュリティ特性を害する試みに対し、AI システムのレジリエンスを確保する上で、重要な役割を果たす。AI システムに対するサイバー攻撃は、訓練用データセット（データポイズニングなど）もしくは訓練済みモデル（アドバーサリアル攻撃やメンバーシップ推論攻撃など）のような AI 固有のリソースを通じておこなわれる可能性があり、または AI システムのデジタルリソースの脆弱性や基盤となる ICT インフラの脆弱性を利用する可能性がある。したがって、リスクに適合したサイバーセキュリティのレベルを確保するため、ハイリスク AI システムの提供者は、必要であれば、基盤となる ICT インフラも考慮しつつ、セキュリティ管理などの適切な対策を講じなければならない。

- (77) 本規則に定める堅牢性および精度に関する要件を害することなく、デジタル要素を含む製品の水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会規則の適用範囲内にあるハイリスク AI システムは、当該規則に従い、当該規則に定める必須のサイバーセキュリティ要件を充足することにより、本規則のサイバーセキュリティ要件を遵守していることを証明することができる。ハイリスク AI システムが、デジタル要素を含む製品に対する水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会規則の必須要件を充足している場合、ハイリスク AI システムは、これらの要件の遵守が EU 適合宣言書または当該規則に基づき発行された宣言書の部分において証明される範囲内において、本規則に定めるサイバーセキュリティ要件を遵守しているとみなされる。このため、デジタル要素を含む製品に対する水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会規則に基づき実施される、本規則に従ってハイリスク AI システムに分類されるデジタル要素を含む製品に関するサイバーセキュリティリスクは、データポイズニングまたは敵対的攻撃などの AI 特有の脆弱性を含む、権限のない第三者によるその使用、その動作またはそのパフォーマンスの変更の試みに関する、AI システムのサイバーレジリエンスに対するリスク、および、必要に応じ、本規則が要求する基本的権利に対するリスクを考慮して評価されなければならない。

- (78) 本規則に定める適合性評価手続きは、デジタル要素を含む製品の水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会規則の対象となるデジタル要素を備える製品で、かつ本規則に基づきハイリスク AI システムに分類される製品の必須のサイバーセキュリティ要件に関連して適用される。しかし、このルール適用は、デジタル要素を含む製品の水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会規則の対象となるデジタル要素を備えた重要な製品について、必要とされる保証レベルの低下を生じさせるものであってはならない。したがって、このルールの適用除外として、本規則の適用範囲にあり、かつデジタル要素を含む製品の水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会の規則に基づきデジタル要素を備えた重要な製品ともみなされるハイリスク AI システムで、本規則の附属書に定める内部統制に基づく適合性評価手続きが適用されるものは、当該規則に定める必須のサイバーセキュリティ要件に関するデジタル要素を備える製品の水平的サイバーセキュリティ要件に関する欧州議会および欧州理事会規則の適合性評価に関する規定の対象となる。この場合、本規則の附属書に定める内部統制に基づく適合性評価に関するそれぞれの規定を、本規則の対象となる他のすべての側面に対し、適用しなければならない。欧州議会および欧州理事会規則(EU)2019/881³⁷に基づき ENISA に委ねられたサイバーセキュリティ政策およびタスクに関する ENISA の知識および専門性に基づき、欧州委員会は AI システムのサイバーセキュリティに関連する問題について、ENISA と協力しなければならない。
- (79) 提供者として定義される特定の自然人または法人は、当該自然人または法人がシステムを設計または開発した者であるかどうかにかかわらず、ハイリスク AI システムの上市またはサービス開始に責任を負うことが適切である。

³⁷ ENISA(欧州情報ネットワーク・セキュリティ機関)および情報通信技術のサイバーセキュリティ認証に関する、ならびに規則(EU)No 526/2013 を廃止する 2019 年 4 月 17 日の欧州議会および欧州理事会規則(EU)2019/881 (サイバーセキュリティ規則) (OJ L 151, 7.6.2019, p.15)。

- (80) EU および加盟国は、国際連合障害者権利条約の締約国として、障害者を差別から保護すること、その平等を促進すること、障害者が他者と等しく情報通信技術および情報通信システムにアクセスできるよう確保すること、ならびに障害者のプライバシーに対する尊重を保証することに対する法的責任を負う。AI システムの重要性と利用が増していることを考慮すると、ユニバーサルデザインの原則をすべての新しい技術およびサービスに適用することは、障害者を含む、AI 技術より潜在的に影響を受けるすべての人またはそれを使用するすべての人に対し、その内在的尊厳およびその内在的多様性を十分に考慮する方法による、完全かつ平等なアクセスを保証しなければならない。したがって、提供者が、欧州議会および理事会指令(EU)2016/2102³⁸ および指令(EU)2019/882 を含む、アクセシビリティ要件を完全に保証することが不可欠である。提供者は、設計段階から、これらの要件の遵守を確保しなければならない。したがって、必要な措置は、ハイリスク AI システムの設計のなかに、可能な限り組み込まなければならない。
- (81) 提供者は、確実な品質管理体制を導入し、必要な適合性評価手続の遵守を確保しようし、関連文書を作成し、かつ確実な市販後モニタリングシステムを導入しなければならない。関連分野の EU 法に基づき品質管理体制に関する義務を負うハイリスク AI システムの提供者は、本規則に定める品質管理体制の要素を、この分野の他の EU 法に定める既存の品質管理体制に組み込む可能性を有する。本規則と既存の分野別の EU 法との補完性は、欧州委員会の将来の標準化活動またはガイダンスにおいても考慮されなければならない。自ら使用することのみを目的とするハイリスク AI システムのサービスを行う公的機関は、分野の特性ならびに関係する公的機関の権限および組織を考慮し、場合により、国レベルまたは地域レベルで採択された品質管理体制の枠内において、品質管理体制に関するルールを採用し、かつ実施することができる。
- (82) 本規則の施行を可能にし、オペレータのために衡平な競争条件を創出するため、かつデジタル製品の利用可能な各種形態を考慮すると、あらゆる状況において、EU 域内に設立された者が、AI システムの適合性に関し、必要なあらゆる情報を当局に対し提供できることを確保することが、重要である。したがって、EU 域内においてその AI システムを利用に供する前に、第三国において設立された提供者は、書面による委任状により、EU 域内で設立された代理人を任命しなければならない。この代理人は、EU 域内に設立されていない提供者が EU 域内に上市またはサービスを開始するハイリスク AI システムの適合性を確保する意味において、かつ提供者の EU 域内に設立された連絡担当者として、極めて重要な役割を果たす。

³⁸ 公共機関のウェブサイトおよびモバイルアプリケーションのアクセシビリティに関する 2016 年 10 月 26 日の欧州議会および欧州理事会指令(EU)2016/2102(OJ L 327, 2.12.2016, p.1)。

- (83) AI システムのバリューチェーンの性質および複雑性を考慮し、新たな立法枠組みに従い、法的安全を保証し、かつ本規則の遵守を促進することが不可欠である。したがって、AI システムの開発に寄与し得る輸入者および頒布者など、当該バリューチェーン全般にわたり関係するオペレータの役割および具体的な義務を明確にする必要がある。一定の状況においては、これらのオペレータは、同時に複数の役割を演じる可能性があり、したがって、これらの役割に結びつくすべての関係する義務を累積的に履行する必要がある。たとえば、オペレータは、同時に、頒布者および輸入者として行動する可能性がある。
- (84) 法的安全を保証するため、一定の特別な条件においては、すべての頒布者、輸入者、導入者またはその他の第三者は、ハイリスク AI システムの提供者と見なされるべきであり、したがって、関係するあらゆる義務を負うことを、明確にする必要がある。これは、この当事者が、義務について別段の割り振りを定める契約上の規定を害することなく、既に上市されまたはサービスが開始されているハイリスク AI システムに、その名またはその商標を付す場合である。この当事者が、既に上市されまたはサービスが開始されているハイリスク AI システムに対し実質的な変更を行い、それが本規則に基づき引き続きハイリスク AI システムである場合、または、ハイリスクに分類されていなかった、既に上市されまたはサービスが開始されている汎用 AI システムを含む AI システムの意図目的を変更し、本規則に従ったハイリスク AI システムになる場合もこれに当たる。これらの規定は、ともに本規則が適用されるべき新たな立法枠組みを前提とする、一定の EU 調和法に定める、より具体的な規定を害することなく適用されなければならない。たとえば、規則 (EU) 2017/745 第 16 条第 2 項は、一定の変更が適用される要件の遵守に対し影響を与える可能性のあるデバイスの変更とみなされるべきではないことを定めているが、当該規則の意味における医療機器を構成するハイリスク AI システムに対し、引き続き適用されなければならない。
- (85) 汎用 AI システムは、それ自体がハイリスク AI システムとして使用されることもあるし、他のハイリスク AI システムのコンポーネントとして使用されることもある。したがって、その特別な性質を理由として、かつ AI バリューチェーン全般にわたる責任の公平な分担を保証するため、当該システムの提供者は、これらのシステムが他の提供者によってそれ自体ハイリスク AI システムとして使用されるか、またはそれがハイリスク AI システムのコンポーネントとして使用されるかを問わず、本規則に別段の定めがない限り、本規則に基づいて設立された管轄当局とともに、本規則に定める関連する義務を関係するハイリスク AI システムの提供者が遵守できるよう、それらと緊密に協力しなければならない。

- (86) 本規則に定める条件のもとで、AI システムを最初に上市し、またはサービスを開始した提供者は、本規則の目的上、もはや提供者とは見なされるべきではなく、この提供者が AI システムをハイリスク AI システムへ変更することを明示的に除外していない場合、この提供者はそれにもかかわらず緊密に協力し、必要な情報を利用可能にし、かつ本規則に定められた義務を遵守するために求められる、特にハイリスク AI システムの適合性評価の遵守に関して求められる、合理的に期待される技術的アクセスおよびその他のあらゆる支援を提供しなければならない。
- (87) さらに、新たな立法枠組みを前提とする EU 調和法の適用範囲内にある製品のセキュリティ・コンポーネントであるハイリスク AI システムが、製品から独立して上市されずまたはサービスが開始されない場合、当該立法が定める製品の製造者は、本規則に定める提供者の義務を遵守しなければならない、かつ、特に、最終製品に組み込まれた AI システムが本規則の要件を遵守していることを保証しなければならない。
- (88) AI バリューチェーン全般にわたり、複数の当事者が AI システム、AI ツール、AI サービスを提供するだけでなく、モデルの訓練、モデルの再訓練、モデルのテストおよび評価、ソフトウェアへの組み込み、またはモデル開発の他の側面を含む、さまざまな目的で、提供者によって AI システムに組み込まれたコンポーネントまたはプロセスも提供する。これらの当事者は、その AI システム、AI ツール、AI サービス、AI コンポーネント、または AI プロセスが搭載されるハイリスク AI システムの提供者に対し、バリューチェーンにおいて果たすべき重要な役割を担い、その知的財産権および営業秘密を害することなく、本規則に定める義務を提供者が完全に遵守できるようにするため、書面による合意により、この提供者に対し、一般的に認められている最先端の技術に基づく、必要な情報、性能、技術的アクセス、およびその他のサポートを提供しなければならない。
- (89) 汎用 AI モデル以外の AI のツール、サービス、プロセス、またはコンポーネントに対し公衆がアクセスできるようにしている第三者は、これらの AI のツール、サービス、プロセスまたはコンポーネントが、フリーかつオープンソースのライセンスのもとでアクセス可能とされている場合、特にそれらを使用または組み込んだ提供者に対し、AI バリューチェーン全般にわたる責任を目的とする要件を遵守する責任を負担させるべきではない。汎用 AI モデル以外の AI のツール、プロセス、またはコンポーネントの開発者は、AI バリューチェーン全般にわたる情報共有を促進するため、モデルカードやデータシートなど、広く採用されているドキュメント実務を実施することが奨励され、それは EU 域内における信頼できる AI システムの促進を可能にする。

- (90) 欧州委員会は、バリューチェーン全般にわたる協力を促進するため、ハイリスク AI システムの提供者と、ハイリスク AI システムに使用されまたは搭載されたツール、サービス、コンポーネントまたはプロセスを提供する第三者との間で定める、自主的なモデル契約条項を作成し、かつ推奨することができる。欧州委員会が、任意のモデル契約条項を作成する場合、特定のセクターまたはビジネスケースにおいて適用され得るあり得る契約上の要件も考慮しなければならない。
- (91) AI システムの性質、およびその使用に潜在的に関係する安全性および基本的権利に対するリスク、特に、実生活の場で AI システムのパフォーマンスの適切なモニタリングを確保する必要性に関し、導入者に対する特別な責任を定めることが適切である。導入者は、特に、それらが使用説明書に従ってハイリスク AI システムを使用することができるように、適切な技術的措置および組織的措置を講じなければならない。必要に応じ、AI システムの動作の監視および記録保存に関し、その他の一定の義務が定められなければならない。さらに、導入者は、本規則に定めるシステムの使用説明書および人間による監督を実行する任務を負う者が、必要な能力、特にこれらの任務を適切に履行するための適切なレベルの AI リテラシー、訓練および権限を備えていることを確保しなければならない。これらの義務は、EU 法または国内法に基づくハイリスク AI システムに関する導入者の他の義務を害してはならない。
- (92) 本規則は、AI システムのサービス開始または使用の決定に関し、欧州議会および欧州理事会指令 2002/14/EC³⁹を含む、EU または国内の法および実務に基づく、雇用者が労働者またはその代表者に通知する義務または通知し諮問する義務を害しない。労働者およびその代表者は、他の法的手段において当該通知義務または通知および諮問義務の条件が満たされていない場合、職場における予定されたハイリスク AI システムの導入について情報を提供されるよう、確保することが依然として必要である。さらに、この情報に対する権利は、本規則の根底にある基本的権利を保護する目的に付随しかつ必要である。したがって、この点に関する情報提供義務は、労働者の既存の権利を害することなく、本規則に定められなければならない。

³⁹ 欧州共同体の従業員に通知しおよび諮問することに関し一般的枠組みを設ける 2002 年 3 月 11 日の欧州議会および欧州理事会指令 2002/14/EC (OJ L 80, 23.3.2002, p.29)。

- (93) AI システムに関係するリスクは、これらのシステムの設計方法から生じ得るが、これらの AI システムの使用方法からも生じ得る。ハイリスク AI システムの導入者は、AI システム開発の際における提供者の義務を補完するので、基本的権利の保護を保証することについて、したがって、重要な役割を果たす。導入者は、ハイリスク AI システムがどのように具体的に使用されることになるかを理解するのに最適な立場にあり、これにより、使用の文脈、および脆弱なグループを含む、影響をうけ得る人または人のグループをより具体的に把握できることから、開発段階では予見されなかった重大な潜在的リスクを特定し得る。本規則の附属書に列挙されるハイリスク AI システムの導入者は、自然人に対する情報提供でも重要な役割を果たし、自然人に関する判断を下す場合、または自然人に関する意思決定を促進する場合、必要に応じ、自然人がハイリスク AI システムの使用の対象となることをその自然人に通知しなければならない。この情報には、システムの意図目的、および下される判断の種類が含まなければならない。また、導入者は、自然人に対し、本規則に定める説明を受ける権利について情報提供しなければならない。法の執行を目的として使用されるハイリスク AI システムについては、この義務は指令(EU)2016/680 第 13 条に従って実施されなければならない。
- (94) 法執行目的の生体認証のための AI システムの使用を前提とする生体データのあらゆる処理は、指令(EU)2016/680 第 10 条を遵守しなければならない。データ主体の権利および自由のため適切なセーフガードを条件として、それが厳密に必要な場合、かつそれが EU 法または加盟国の法により許可される場合にのみ、当該処理が許可される。当該使用は、それが許可される場合、特に、合法性、公平性、透明性、目的の制限、精度、保管の制限など、指令(EU) 2016/680 第 4 条第 1 項に定める原則も尊重するものでなければならない。
- (95) 適用される EU 法、特に規則(EU)2016/679 および指令(EU)2016/680 を害することなく、事後的遠隔生体認証システムの介入的性質を考慮し、事後的遠隔生体認証システムの使用は、セーフガードの対象としなければならない。事後的遠隔生体認証システムは、常に、相応で、合法的で、厳密に必要な方法で使用されなければならない。したがって、識別される者、場所、時間的範囲に関して、合法的に取得されたビデオ映像のクローズドなデータセットに基づき、ターゲットを絞られなければならない。いずれにせよ、事後的遠隔生体認証システムは、無差別な監視を行うために、法執行行為の枠組みにおいて用いられてはならない。事後的遠隔生体認証システムの条件は、いかなる場合においても、リアルタイム遠隔生体認証のために、禁止の条件および厳格な例外を回避できる根拠を提供するものであってはならない。

(96) 基本的権利の保護を効果的に保証するため、公法上の組織または公共サービスを提供する民間の主体であるハイリスク AI システムの導入者、および銀行業者または保険業者など、本規則の附属書に列挙する一定のハイリスク AI システムの導入者は、サービス開始前にこれらのシステムの基本的権利に関する影響分析を実施しなければならない。人にとって重要な公共サービスは、民間の主体によっても提供され得る。このような公共サービスを提供する民間の主体は、教育、医療、社会サービス、住宅および司法行政などの分野における、公共の利益の任務に関係する。基本的権利に関する影響分析は、関係し得る人または人のグループの権利に対する具体的リスクを導入者が特定すること、およびこれらのリスクが現実化した場合に講じるべき措置を導入者が特定することを目的とする。影響分析は、ハイリスク AI システムの最初の導入前に実施され、かつ導入者が関連する要因のいずれかが変更されたと判断する場合にアップデートされなければならない。影響分析は、ハイリスク AI システムがその意図目的に従って使用されるなかで、導入者の関連プロセスを特定し、かつ、システムが使用されることを目的とする期間および頻度、ならびに特定の使用状況において関係し得る特定のカテゴリの自然人およびグループを示さなければならない。

この分析は、これらの人またはグループの基本的権利に対し影響を与え得る害の特定のリスクの識別も含まなければならない。この分析を実施する際、導入者は、ハイリスク AI システムの提供者が使用説明書において提供した情報を含むが、これに限ることなく、影響の適切な分析に関する情報を考慮しなければならない。導入者は、特定されたリスクに照らし、これらのリスクが具体化した場合に講じるべき措置を決定しなければならない。これには、例えば、使用説明書に従った人間による管理に関する取決め、または苦情処理手続きおよび救済手続きなどの、特定の使用状況におけるガバナンスに関する取決めを含み、それらは具体的なユースケースにおける基本的権利に対するリスクを軽減することに貢献し得る。この影響分析を実行した後、導入者は、関係する市場監視当局にそれを通知しなければならない。必要に応じ、影響分析の実施に必要な関連情報を収集するため、ハイリスク AI システムの導入者は、特に AI システムが公のセクターにおいて使用される場合、AI システムによって影響を受ける可能性のある人のグループの代表者、独立の専門家、市民社会組織を含む、関係するステークホルダーを、この影響分析の実施、およびリスクが具体化した場合に講じるべき措置の設計に関与させることができる。欧州人工知能事務局(以下「AI オフィス」という)は、コンプライアンスを促進し、かつ導入者の管理上の負担を軽減するため、質問事項のテンプレートを作成しなければならない。

(97) 汎用 AI モデルの概念は、法的安全を保証するため、明確に定義され、かつ AI システムの概念と区別されなければならない。当該定義は、汎用 AI モデルの主な機能上の特性、特に、汎用性および幅広い範囲の異なるタスクを適切に実行する性能に基づくものでなければならない。これらのモデルは、自己教師あり学習、教師なし学習、強化学習など、各種の方法により、一般に、大量のデータで訓練される。汎用 AI モデルは、特に、ライブラリ、アプリケーション・プログラミング・インターフェース(API)、直接的なダウンロード、物理的コピーなど、様々な方法により上市され得る。これらのモデルは、新しいモデルにさらに変更されまたはファイン・チューニングされ得る。AI モデルが AI システムに不可欠なコンポーネントであるとしても、それ自体では AI システムを構成しない。AI モデルが AI システムになるには、ユーザーインターフェースなど他のコンポーネントをそれに追加する必要がある。AI モデルは、一般に、AI システムに搭載され、その一部を構成する。本規則は、汎用 AI モデルおよびシステムック・リスクを示す汎用 AI モデルについて、特別なルールを定めるものであり、これらのモデルが AI システムに組み込まれまたは AI システムの一部を構成する場合にも適用されなければならない。汎用 AI モデルの提供者に課される義務は、ひとたびこれらのモデルが上市されれば適用されると考えることが適切である。

汎用 AI モデルの提供者が、市場において利用に供しまたはサービスを開始するその固有の AI システムに、固有のモデルを組み込む場合、このモデルは上市されたと見なされなければならない。したがって、モデルについて本規則に定める義務は、AI システムに適用される義務に加えて、引き続き適用されなければならない。モデルについて定められる義務は、いかなる場合も、固有のモデルが、製品またはサービスを第三者に提供するために不可欠ではなく、かつ自然人の権利に影響を与えない、純粋に内部プロセスのために使われる場合には、適用されない。その著しい潜在的悪影響を考慮すると、システムック・リスクを示す汎用 AI モデルは、常に、本規則に定める関連する義務の対象とされなければならない。当該定義は、研究、開発および試作の各活動のみを目的として上市前に使用される AI モデルを対象としない。当該活動に続いてモデルが上市される場合、本規則を遵守する義務を害しない。

- (98) モデルの汎用性は、とりわけ、多数のパラメータによっても決定され得るが、少なくとも 10 億のパラメータを持ち、大規模な自己教師あり学習を用いて大量のデータで訓練されたモデルは、著しい汎用性を示し、幅広い範囲の異なるタスクを適切に実行するものとみなされなければならない。
- (99) 大規模生成 AI モデルは、テキスト、音声、画像または映像など、コンテンツを柔軟に生成でき、幅広い範囲の異なるタスクに容易に適応できるものであるから、汎用 AI モデルの典型例である。
- (100) 汎用 AI モデルが、AI システムに組み込まれ、または AI システムの一部を構成する形成する場合、この組み込みにより、このシステムがさまざまな目的に対応する性能を有するならば、このシステムは汎用 AI システムと見なされなければならない。汎用 AI システムは、直接的に使用されることも、または他の AI システムに組み込まれることもあり得る。
- (101) 汎用 AI モデルの提供者は、これらのモデルをその製品に組み込むことができ、同時に、本規則またはその他の規則に基づき課せられる義務を履行するため、その提供するモデルが、モデルとその性能を適切に理解する必要がある川下の提供者によって提供されることがある、一連の川下のシステムの基礎を構成しようとする理由により、AI バリューチェーン全般にわたり、特別な役割および責任がある。したがって、文書の作成と最新の状態の維持、および川下の提供者による使用のための汎用 AI モデルに関する情報の提供を含む、相応の透明性措置が定められなければならない。技術文書は、請求により、AI オフィスおよび各国の所轄当局の利用に供され得るよう、汎用 AI モデルの提供者が作成し、最新の状況に保たれなければならない。この文書に含まれるべき一連の最小限の要素は、本規則の特定の附属書に記載されなければならない。欧州委員会は、技術の発展に照らし、委任法令により、これらの附属書を改正する権限が与えられなければならない。
- (102) フリーかつオープンソースのライセンスの枠内においてリリースされるモデルを含む、ソフトウェアおよびデータで、自由に共有され得、かつ、ユーザーが、これらのソフトウェアおよびデータまたはそれらの修正版を自由に参照し、使用し、変更し、再頒布できるものは、市場における研究およびイノベーションに寄与し得るし、EU 経済に重要な成長の機会を与え得る。フリーかつオープンソースのライセンスのもとでリリースされる汎用 AI モデルは、重み、モデルアーキテクチャに関する情報、およびモデルの使用に関する情報を含む、パラメータが公開されている場合には、ハイレベルな透明性および公開性が保証されているものとみなされる。当該ライセンスは、当初のモデル提供者が記載され、同一または同等の頒布条件が遵守されることを条件として、ユーザーが、モデルを含むソフトウェアおよびデータを、利用し、コピーし、頒布し、研究し、変更し、および改善することができる場合にも、フリーかつオープンソースであるとみなされる。

- (103) フリーかつオープンソースの AI コンポーネントは、モデルおよび汎用 AI モデル、AI システムのツール、サービスまたはプロセスを含む、ソフトウェアおよびデータを対象とする。フリーかつオープンソースの AI コンポーネントは、オープンリポジトリにおけるその開発を含む、さまざまなチャネルにより提供され得る。本規則の適用上、支払いを受けてまたは他の対価を受けて提供される AI コンポーネントは、特にソフトウェアのプラットフォームによる AI コンポーネントに関する技術支援またはその他のサービスの提供、または、零細企業間の取引を除き、ソフトウェアのセキュリティ、互換性、相互運用性の向上のみを目的とするもの以外の理由により個人データを使用することを含め、フリーかつオープンソースの AI コンポーネントについて定める例外を享受するものであってはならない。オープンリポジトリによる AI コンポーネントの利用の提供は、それ自体として対価性を構成するものではない。
- (104) フリーかつオープンソースのライセンスのもとでリリースされ、その重み、モデルのアーキテクチャに関する情報およびモデルの使用に関する情報を含む、パラメータが公開されている汎用 AI モデルの提供者は、汎用 AI モデルに課せられる透明性の要件に関する例外の対象となる。それは、そのモデルがシステミック・リスクを示すとみなされ得ない限りであり、この場合、モデルに透明性があり、オープンソースライセンスを伴うという事実は、本規則に定める義務の遵守を除外する十分な理由とはみなされない。いずれにせよ、フリーかつオープンソースのライセンスのもとでの汎用 AI モデルのリリースは、モデルの訓練またはファイン・チューニングに使用されたデータセットに関する重要な情報、およびそれによって著作権法の遵守がどのように確保されているかに関する重要な情報が、必ずしも明らかにされるものではないことから、透明性の要件の遵守に関し汎用 AI モデルについて定める例外は、モデルの訓練のために使用されたコンテンツの要約を作成する義務にも、特に欧州議会および欧州理事会指令(EU)2019/790⁴⁰第 4 条第 3 項に基づく権利の留保を特定してかつ遵守する、著作権に関する EU 法を遵守することを目的とするポリシーを実施する義務にも関係しない。

⁴⁰ デジタル単一市場における著作権および隣接権に関するならびに指令 96/9 / EC および 2001/29 / EC を修正する 2019 年 4 月 17 日の欧州議会および欧州理事会指令 (EU) 2019/790 (OJ L 130, 17.5.2019, p.92)。

- (105) 汎用 AI モデル、特にテキスト、画像、その他のコンテンツを生成できる大規模生成 AI モデルは、ユニークなイノベーションの機会となるだけでなく、アーティスト、作家、その他のクリエイター、およびその創作的コンテンツの作成、頒布、使用、消費の方法に対する課題も示す。これらのモデルの開発および訓練には、膨大な量のテキスト、画像、ビデオ、およびその他のデータへのアクセスを必要とする。テキストマイニングおよびデータマイニング技術は、著作権および著作隣接権によって保護され得るこれらのコンテンツの抽出および分析のために、この文脈において広く使用され得る。著作権により保護されたコンテンツのあらゆる使用は、関連する著作権に関する例外および制限が適用されない限り、関係する権利者の許諾が必要である。指令 (EU)2019/790 は、一定の条件のもとで、テキストマイニングおよびデータマイニングの目的で、著作物またはその他の保護対象物の複製および抽出を認める例外および制限を導入した。これらのルールに基づき、権利者は、学術研究目的で行われるものでない限り、テキストマイニングおよびデータマイニングを回避するため、著作物またはその他の保護対象物に対する権利を留保することを選択することができる。オプトアウトの権利が適切な方法により明示的に留保されている場合、汎用 AI モデルの提供者は、これらの著作物に対しテキストマイニングおよびデータマイニングの実行を希望するのであれば、権利者から許諾を得なければならない。
- (106) 汎用 AI モデルを EU 市場に上市する提供者は、本規則に定める関連する義務の遵守を確保しなければならない。このために、汎用 AI モデルの提供者は、著作権および著作隣接権に関する EU 法を遵守するためのポリシー、特に指令(EU)2019/790 第 4 条第 3 項に従い権利者が表明した権利の留保を特定しかつ遵守するためのポリシーを確立しなければならない。汎用 AI モデルを EU 市場に上市する提供者はすべて、これらの汎用 AI モデルの訓練の基礎となる著作権に関する行為が展開される裁判管轄に関係なく、この義務を遵守しなければならない。これは、汎用 AI モデルの提供者間における衡平な競争条件を保証するために必要であり、そこではいかなる提供者も、EU 域内で定められる著作権のルールよりも低い著作権のルールを適用することにより、EU 市場において競争上の優位を得ることはできない。
- (107) 著作権法により保護されるテキストおよびデータを含め、汎用 AI モデルの事前学習および訓練の枠内で使用されるデータに関する透明性を高めるため、これらのモデルの提供者は、汎用 AI モデルの訓練のために用いられたコンテンツの十分に詳細な要約を作成し、公衆の利用に供することが適切である。営業秘密および秘密情報を保護する必要性を十分に考慮し、この要約は、著作権者を含む正当な利益を有する当事者が、EU 法がそれらに与えた権利を行使しおよび遵守させることを容易にするため、たとえば、大規模な公私のデータアーカイブまたはデータベースのような、モデルの訓練のために使用された主なデータセットまたはデータ集合物を挙げたり、使用された他のデータソースに関する説明文を提供したりするなどであり、技術的な面について詳述するというより、内容に関して全般的に包括するものでなければならない。AI オフィスは、シンプルかつ有用で、提供者が必要な要約を記述形式で提供できる、要約のテンプレートを提供することが適切である。

- (108) 汎用 AI モデルの提供者に課せられる、著作権に関する EU 法を遵守するためのポリシーを確立する義務、および訓練のために使用されたコンテンツの要約を公衆の利用に供する義務について、AI オフィスは、著作権の遵守に関し、訓練データの著作物ごとの検証または評価をおこなうことなく、提供者がこの義務を履行しているかどうかを検証しなければならない。本規則は、EU 法に定める著作権に関するルールの適用に影響しない。
- (109) 汎用 AI モデルの提供者に適用される義務の遵守は、モデルの提供者のタイプに対応しかつ相応ものでなければならず、業務外の目的または学術研究目的でモデルを開発または使用する者が遵守することは必要ではないが、それにもかかわらず、これらの者はこれらの要件を自発的に遵守することが奨励される。著作権に関する EU 法を害することなく、これらの義務の遵守は、提供者の規模を十分に考慮し、スタートアップを含む中小企業が、過度のコストを体現することなくかつ当該モデルの使用を思いとどまらせることのない、簡素化された遵守の手段を用いることができるようにしなければならない。モデルの変更またはファイン・チューニングの場合、汎用 AI モデルの提供者に課せられる義務は、この変更またはこのファイン・チューニングに限られなければならない。たとえば、本規則に定めるバリューチェーンに関する義務を遵守するため、訓練データの新たなソースを含む、変更に関する情報によって既存の技術文書を補完することによることなどである。

- (110) 汎用 AI モデルは、システムック・リスクを示す可能性がある。それは、重大事故、重要セクターの混乱、ならびに公衆衛生および公共の安全に対する重大な結果に関連する、現実のまたは合理的に予見可能なあらゆる悪影響、民主的プロセス、公共の安全および経済安全保障に対する現実のまたは合理的に予見可能なあらゆる悪影響、ならびに違法、虚偽、または差別的なコンテンツの拡散を含むが、これらに限定されない。システムック・リスクは、モデルの性能およびモデルの範囲に伴って増加するものと理解されるべきであり、モデルのライフサイクル全般にわたり生じる可能性があり、かつ誤用の条件、モデルの信頼性、モデルの公平性およびモデルのセキュリティ、モデルの自律性のレベル、ツールに対するアクセス、新規のまたは組み合わせられたモダリティ、リリースおよび頒布の戦略、ガードレール除去の可能性、およびその他の要因により影響を受ける。特に、国際的なアプローチは、これまでのところ、リスクに注意を払う必要性を明確にしており、そのリスクは次のものである。潜在的な意図的誤用、または人間の意図とのアラインメントに関連する意図しない制御の問題；兵器の開発、設計、取得または使用の目的を含む、導入の障壁を下げる方法などのような、化学、生物、放射性物質および核のリスク；脆弱性の発見、脆弱性の悪用、または脆弱性の作戦使用を可能とする方法など、サイバー攻撃能力；たとえば、物理システムを制御する能力および重要インフラに干渉する能力を含む、相互作用およびツールの使用の影響；モデルがそれ自身のコピーを作成する可能性、または他のモデルを「自己複製」させもしくは訓練するリスク；モデルが、個人、コミュニティまたは社会に対するリスクを示す、有害な偏見および差別を生じさせ得る方法；民主的価値および人権に対する脅威による、偽情報の助長またはプライバシー侵害；特別な事象が、都市全体、活動分野全体、またはコミュニティ全体にまで影響を与え得る重大な悪影響をもたらす連鎖反応を引き起こすリスク。

(111) 汎用 AI モデルをシステミック・リスクのある汎用 AI モデルとして分類する方法論を確立することが適切である。システミック・リスクは特に高度な性能から生じるため、汎用 AI モデルは、適切な方法論および技術的ツールに基づいて評価されるハイインパクトの性能がある場合、またはその範囲により域内市場に重大な影響を与える場合、システミック・リスクを示すとみなされなければならない。汎用 AI モデルにおけるハイインパクトの性能とは、最先端の汎用 AI モデルに記録された性能と同等またはそれを上回る性能をいう。モデルの性能の全容は、上市後、または導入者がモデルと協働する場合に、より理解され得る。本規則の発効時点の最新技術によれば、浮動小数点演算により測定される汎用 AI モデルの訓練に使用される累積計算量は、モデルの性能の関連する近似値の 1 つである。訓練に使用される累積計算量には、事前訓練、合成データ生成、ファイン・チューニングのような、導入前にモデルの性能を強化することを目的としたアクティビティおよびメソッド全体について使用される計算が含まれる。したがって、浮動小数点演算の初期閾値を設定することが適切であり、それは汎用 AI モデルがそれに達する場合、汎用 AI モデルがシステミック・リスクを示すものであるとの推定を導く。この閾値は、アルゴリズムの改善またはハードウェアの効率性の向上のような、技術上および産業上の変革を考慮するため、時間の経過に伴い調整されなければならない、かつモデルの性能の指標およびベンチマークにより補完されなければならない。

このため、AI オフィスは、学会、産業界、市民社会、その他の専門家と協力しなければならない。閾値、ならびにハイインパクトの性能を評価するためのツールおよびベンチマークは、汎用 AI モデルの汎用性およびその性能、ならびにそれに関連するシステミック・リスクの適切な指標でなければならない、かつモデルが上市される方法および影響を与え得るユーザー数を考慮に入れることができる。この体制を補完するため、欧州委員会は、汎用 AI モデルが設定された閾値を前提とする性能または影響と同等の性能または影響を有することを確認した場合、この汎用 AI モデルがシステミック・リスクを示す汎用 AI モデルであると指定する個別の決定を下す可能性がある。この決定は、訓練データセットの質または規模、モデルのビジネスユーザー数およびエンドユーザー数、その入力および出力のモダリティ、自律性および拡張性のレベル、またはアクセスできるツールのような、本規則の附属書に定めるシステミック・リスクを示す汎用 AI モデルの指定基準の全体的な評価に基づき、下されなければならない。システミック・リスクを示す汎用 AI モデルである指定されたモデルの提供者の理由を示した請求があった場合、欧州委員会は当該要求を考慮しなければならない、かつ汎用 AI モデルが依然としてシステミック・リスクを示すと見なし得るかどうか再評価する決定をすることができる。

- (112) システミック・リスクを示す汎用 AI モデルの分類手続きを明確に確立することも、また必要である。ハイインパクトの性能について、適用される閾値に達する汎用 AI モデルは、システミック・リスクを示す汎用 AI モデルであると推定されるべきである。提供者は、要件が充足された後、または汎用 AI モデルが推定を導く要件を充足していることが判明した後、遅くとも 2 週間以内に、AI オフィスに通知しなければならない。これは浮動小数点演算の閾値に特に関連する。汎用 AI モデルの訓練は、コンピューティングリソースの事前割り当てを含む、相当な計画が必要であり、したがって、汎用 AI モデルの提供者は、訓練が完了する前に、そのモデルが閾値に達しているかどうかを知ることができるからである。この通知の枠内において、提供者は、それらの特別な性格を理由として、汎用 AI モデルが例外的にシステミック・リスクを示さないこと、したがってシステミック・リスクを示す汎用 AI モデルとして分類されないことを、証明することができなければならない。これらの情報の要素は、システミック・リスクを示す汎用 AI モデルの上市に、AI オフィスが、あらかじめ備えることを可能とする点で、AI オフィスにとって有用であり、したがって、提供者は、早い段階で、AI オフィスとの協力を開始することができる。オープンソースモデルのリリース後、本規則に定める義務の遵守を保証するために必要な措置は、実施がより困難になり得ることから、オープンソースとしてリリースされる予定の汎用 AI モデルに関しては、当該情報は特に重要である。
- (113) 欧州委員会は、汎用 AI モデルが、システミック・リスクを示す汎用 AI モデルとして分類するための要件を充足し、以前は知られていなかった、または関係する提供者が欧州委員会に通知しなかった事実を知った場合、当該モデルをそのように指定する権限を有するものでなければならない。適格な警告システムは、AI オフィスが、そのモニタリング活動に加え、学術パネルにより、システミック・リスクを示す汎用 AI モデルとして分類されるべき汎用 AI モデルについて通知されるように保証するものでなければならない。
- (114) システミック・リスクを示す汎用 AI モデルの提供者は、汎用 AI モデルの提供者について定める義務だけでなく、問題のモデルがスタンドアロンモデルとして提供されるか、または AI システムまたは AI 製品に組み込まれているかを問わず、これらのリスクを特定しかつ軽減すること、および適切なレベルのサイバーセキュリティの保護を保証することを目的とする義務を負わなければならない。これらの目的を達成するため、本規則は、提供者に対し、提供者が、特にその最初の上市前に、モデルのアドバーサリアルテストの実施および文書化、および、必要に応じ、内部のまたは独立した外部のテストにより、必要なモデルの評価を実施することを要求する。さらに、システミック・リスクを示す汎用 AI モデルの提供者は、例えば、説明責任やガバナンスのプロセスのようなリスク管理ポリシーの導入、市販後モニタリングの実施、モデルのライフサイクル全般にわたる適切な措置の実施、AI バリューチェーン全般にわたる関係当事者との協力など、システミック・リスクを継続的に評価しかつ軽減しなければならない。

- (115) システミック・リスクを示す汎用 AI モデルの提供者は、潜在的システミック・リスクを評価しかつ軽減しなければならない。システミック・リスクを示しうる汎用 AI モデルに関連するリスクを特定しかつ防止するための努力にもかかわらず、モデルの開発または使用が重大インシデントを引き起こした場合、汎用 AI モデルの提供者は、不当に遅滞することなく、インシデントの追跡を実施し、あらゆる関連情報および可能な是正措置を欧州委員会および各国の所轄当局に通知しなければならない。さらに、提供者は、必要に応じ、モデルのライフサイクル全体にわたり、モデルおよびその物理的インフラに関し、適切なレベルのサイバーセキュリティの保護を保証しなければならない。悪意のある使用または攻撃に関連するシステミック・リスクに対抗するサイバーセキュリティの保護は、モデルの偶発的な漏洩、許諾のないリリース、セキュリティ対策の回避、およびサイバー攻撃、不正アクセスまたはモデルの盗難に対する防御を、十分に考慮しなければならない。そのような保護は、特に、関連する状況および問題のリスクに適した、情報セキュリティ、特別なサイバーセキュリティポリシー、適切に確立された技術的ソリューション、物理的なまたは情報処理上のアクセスコントロールなどを通じ、モデルの重み、アルゴリズム、サーバー、およびデータセットをセキュアなものとすることによって、促進され得る。
- (116) AI オフィスは、国際的なアプローチを考慮しつつ、行動規範の策定、再検証、適用を奨励し、促進しなければならない。汎用 AI モデルのすべての提供者は参加を求められ得る。行動規範が最先端技術に対応し、かつ多様な視点全体を十分に考慮することを確保するため、AI オフィスは関係する各国の所轄当局と協力し、必要に応じ、この規範を策定するため、市民社会組織、特に学術団体を含むその他の関係するステークホルダーおよび関係の専門家に諮問しなければならない。行動規範は、汎用 AI モデルおよびシステミック・リスクを示す汎用 AI モデルの提供者に課す義務を取り扱うものでなければならない。さらに、システミック・リスクに関し、行動規範は、その発生源を含む、EU レベルでのシステミック・リスクの種類および性質のリスク分類の確立に貢献するものでなければならない。行動規範は、また、特定のリスク評価および軽減策について焦点を当てるものでなければならない。

(117) 行動規範は、本規則に基づき汎用 AI モデルの提供者に課せられる義務が適切に遵守されるための、中心的なツールでなければならない。提供者は、その義務を遵守していることを証明するため、行動規範を根拠とすることができる。欧州委員会は、実施法令により、行動規範を承認すること、かつそれに EU 域内における一般的な有効性を付与することができ、または、その代わりに、本規則が適用されるようになる前に行動規範を完成させることができない場合か、または当該規範を AI オフィスにより適切とみなされない場合には、関連する義務の履行のための共通ルールを定めることを決定することができる。統一規格が公表され、AI オフィスにより関連する義務を適切にカバーしていると評価される場合、提供者は、欧州統一規格を遵守する場合に、適合性の推定を受ける。さらに、汎用 AI モデルの提供者は、行動規範もしくは統一規格がない場合、またはそれらに依拠しないことを選択した場合に、適切な代替手段を使用して、適合性を証明することができる。

(118) 本規則は、規則(EU)2022/2065 の対象となるそのサービスに AI システムおよび AI モデルを組み込む仲介サービス提供者に課される義務を補完しつつ、EU 域内において AI システムおよび AI モデルを上市し、サービスを開始または使用する関連市場の行為者を対象として、一定の要件および義務を課すことにより、AI システムおよび AI モデルを規制する。これらのシステムまたはモデルが、非常に大規模なオンラインプラットフォームまたは非常に大規模なオンライン検索エンジンに組み込まれている限り、規則(EU)2022/2065 に定めるリスク管理フレームワークの対象となる。したがって、規則(EU)2022/2065 の対象でない重大なシステム・リスクが生じない限り、かつそのようなモデルにおいて特定されない限り、本規則の対応する義務は履行されていると推定されなければならない。このフレームワークにおいて、非常に大規模なオンラインプラットフォームおよび非常に大規模なオンライン検索エンジンの提供者は、サービスにおいて使用されるアルゴリズムのシステム設計が、これらのリスクおよび潜在的な誤用から生じるシステム・リスクをどのように助長するかを含め、そのサービスの設計、動作、および使用から生じるシステム・リスクを評価する義務を負う。また、これらの提供者は、基本的権利の遵守を確保するために、適切な緩和措置を講じる義務を負う。

(119) EU法のさまざまな法文の適用範囲に関するデジタルサービスのイノベーションと技術的進展の急速なペースを考慮すると、特にその名宛人の使用と理解に照らし、本規則により規制される AI システムは、規則(EU)2022/2065 にいう仲介サービスまたはその一部として提供され得るものであり、これは技術的に中立な方法で解釈されなければならない。例えば、特に、チャットボットのような AI システムが、原則として、あらゆる Web サイトにおいて検索を実行し、次に検索結果をその既存の知識に組み込み、かつ異なる情報源を組み合わせることで単一の出力を生成するようにアップデートされた知識を使用する範囲内において、AI システムは、オンライン検索エンジンを提供するために、使用され得る。

(120) さらに、一定の AI システムにより生じる出力が、AI により生成されまたは操作されていることを検出しおよび開示できるようにするため、本規則に基づき一定の AI システムの提供者および導入者に課せられた義務は、規則(EU)2022/2065 の効果的な実施を促進することについて、特別な重要性を有する。これは、AI よりに生成されまたは操作されたコンテンツの拡散から生じ得るシステムック・リスクを特定しかつ軽減するために、非常に大規模なオンラインプラットフォームまたは非常に大規模なオンライン検索エンジンの提供者に課せられる義務に対して適用される。リスクは、特に、偽情報によることを含む、民主的プロセス、公の言論および選挙プロセスにおいて、現実のまたは予見可能な悪影響のリスクである。

(121) 標準化は、最先端の技術に従って本規則の遵守を保証する目的で、および単一市場におけるイノベーション、競争力および成長性を促進する目的で、提供者に対し、技術的ソリューションを提供するため、重要な役割を果たすものでなければならない。欧州議会および欧州理事会規則(EU)No 1025/2012⁴¹第 2 条(1)(c)に定義されるような統一規格は、通常、最先端の技術を考慮すべきものであり、統一規格の遵守は、提供者が本規則の要件を遵守していることを証明する手段となるものでなければならない。したがって、規則(EU)No 1025/2012 第 5 条および第 6 条に従って、規格の策定に関係するすべてのステークホルダー、特に中小企業、消費者団体ならびに、環境および社会的ステークホルダーなどが関与する、均衡の取れた利益の代表が奨励されることが適切である。コンプライアンス促進のため、標準化の請求は、欧州委員会により、不当に遅延することなく、提出されなければならない。標準化の請求を作成する際、欧州委員会は、関係する専門知識を収集するため、アドバイザー・フォーラムおよび AI 委員会に諮問しなければならない。しかし、統一規格に関する参照情報がない場合、欧州委員会は、実施法令により、アドバイザー・フォーラムへの諮問後、本規則に基づく一定の要件の共通仕様を作成することができる。

共通仕様は、標準化の請求が欧州標準化機関のいずれからも受理されなかった場合、関連する統一規格が基本的権利の分野における懸念に対し十分に対応していない場合、統一規格が請求に適合していない場合、または適切な統一規格の採用が遅れている場合に、本規則の要件を遵守する提供者の義務を促進するための例外的なフォールバック・ソリューションでなければならない。統一規格のそのような採用の遅れが、当該規格の技術的複雑性によるものである場合、欧州委員会は、共通仕様の確立を検討する前に、それを考慮しなければならない。欧州委員会が共通仕様を策定する場合、国際的なパートナーおよび国際標準化団体と協力することが推奨される。

⁴¹ 欧州標準化に関する、ならびに欧州理事会指令 89/686/EEC および 93/15/EEC、ならびに欧州議会および欧州理事会指令 94/9/EC、94/25/EC、95/16/EC、97/23/EC、98/34/EC、2004/22/EC、2007/23/EC、2009/23/EC および 2009/105/EC を改正する、ならびに欧州理事会決定 87/95/EEC および欧州議会および欧州理事会決定 No 1673/2006/EC を廃止する、2012 年 10 月 25 日の欧州議会および欧州理事会規則(EU)No 1025/2012、(OJ L 316, 14.11.2012, p12)。

- (122) 統一規格および共通仕様の使用を害することなく、AI システムを使用することを目的とする一定の地理的、行動的、文脈的または機能的範囲設定を反映するデータによって訓練されおよびテストされたハイリスク AI システムの提供者は、本規則に定めるデータガバナンスに関する要件に基づき定める関連措置を遵守していると推定されることが適切である。本規則に定める堅牢性および精度に関する要件を害することなく、規則(EU)2019/881 第 54 条第 3 項に従い、同規則に基づきサイバーセキュリティのスキームの範囲内で認証され、または適合宣言書が発行され、かつ EU 官報にその参照情報が掲載されたハイリスク AI システムは、サイバーセキュリティ証明書もしくは適合宣言書、またはそれらの一部が本規則のサイバーセキュリティ要件を対象としている限り、本規則のサイバーセキュリティ要件を遵守していると推定されなければならない。これは、当該サイバーセキュリティのスキームが任意である性質を害するものではない。
- (123) ハイリスク AI システムのハイレベルな信頼性を保証するため、これらのシステムは、上市またはサービス開始前に、適合性評価を受けなければならない。
- (124) オペレータにかかる負担を最小限に減らし、かつ重複の可能性を回避するため、新たな立法枠組みに基づく既存の EU 調和法の対象となる製品に関するハイリスク AI システムの本規則の要件への適合性は、この法に基づき既に定められている適合性評価の枠内において評価されなければならない。したがって、本規則の要件の適用可能性は、関連する EU 調和法に基づく適合性評価に特有の論理、方法論、または一般的な構造に影響を与えない。
- (125) ハイリスク AI システムの複雑性およびそれらに関連するリスクを考慮し、認証機関が関与するこれらのシステムのための適切な適合性評価手続き、つまり「第三者適合性評価」を策定することが重要である。しかし、製品の安全性の分野における上市前の専門の認証機関の現在の経験および、関連するリスクのさまざまな性質を考慮し、少なくとも本規則の適用の初期段階においては、製品に関するハイリスク AI システム以外のハイリスク AI システムに対し、第三者により実施される適合性評価の適用範囲を制限することが適切である。したがって、これらのシステムの適合性評価は、生体認証のために使用されることを目的とする AI システムのみを除き、原則として提供者により提供者自身の責任のもとで実施されなければならない。

- (126) 必要に応じ、第三者による適合性評価を実施するため、認証機関は、特に、独立性、能力、利益相反がないことに関する要件全般、および適切なサイバーセキュリティ要件について、一連の要件を充足していることを条件とし、各国の所轄当局により、本規則に基づき通知されなければならない。これらの機関の通知は、決定 768/2008/EC の附属書 I 第 R23 条に従って、欧州委員会が開発しかつ管理する電子通知ツールにより、各国の所轄当局から欧州委員会および他の加盟国に送付されなければならない。
- (127) 貿易の技術的障壁に関する世界貿易機関の協定に基づく EU のコミットメントに従い、第三国の法律に基づき設立された適合性評価機関が本規則に基づき適用される要件を充足していること、および EU がこの範囲で協定を締結していることを条件として、適合性評価機関が設立されている領土とは独立して、管轄の適合性評価機関が行った適合性評価の結果の相互承認を促進することが適切である。この文脈において、欧州委員会は、そのために国際的手段の可能性を積極的に検討し、かつ、特に第三国との相互承認協定の締結の実現に努めなければならない。
- (128) EU 調和法により規制される製品について実質的な変更という共通して定められた概念に従って、ハイリスク AI システムの本規則に対する適合性に対して影響を与える可能性のある変更（たとえば、オペレーティングシステムまたはソフトウェアアーキテクチャの変更）が生じるとに、またはシステムの意図目的が変更されるごとに、当該 AI システムは、新たな適合性評価手続きの対象となる新たな AI システムと見なすことが適切である。しかし、上市后またはサービス開始後に「学習」し続ける AI システムのアルゴリズムおよびパフォーマンスに生じる変更、すなわち、機能の実行方法の自動的適応は、これらの変更が提供者によって事前に決定され、かつ適合性評価の時点で評価されていることを条件として、実質的な変更を構成しない。
- (129) ハイリスク AI システムが域内市場において自由に移動できるよう、本規則へのその適合性を示す CE マーキングがハイリスク AI システムに貼付されなければならない。製品に組み込まれたハイリスク AI システムについては、物理的な CE マーキングが貼付されなければならない。必要に応じ、デジタル CE マーキングにより補完される。デジタル形式でのみ提供されるハイリスク AI システムについては、デジタル CE マーキングを使用することが適切である。加盟国は、本規則に定める要件を充足し、かつ、CE マーキングが付されたハイリスク AI システムの上市またはサービス開始に、不当な障害を生じさせてはならない。

(130) 一定の条件の下において、革新的な技術の迅速な利用可能性は、人の健康および安全、環境保護および気候変動対策、ならびに社会全体のために、重要となり得る。したがって、公共の安全もしくは自然人の生命および健康の保護、環境保護および重要な産業資産および重要インフラの保護に関連する例外的な理由のため、市場監視当局が、適合性評価の対象となっていない AI システムの上市またはサービス開始を許可できることが適切である。本規則に定める十分に正当化される状況において、法執行機関または市民保護当局は、この許可が使用中または使用後に不当に遅延することなく請求されることを条件として、市場監視当局の許可を得ることなく、特定のハイリスク AI システムのサービスを開始することができる。

(131) AI 分野における欧州委員会および加盟国の業務を促進するため、かつ公衆に対する透明性を高めるため、当該分野における既存の EU 調和法の適用範囲内にある製品に関連するもの以外のハイリスク AI システムの提供者、および本規則の附属書においてハイリスクのユースケースのリストに記載される AI システムが適用除外に基づきハイリスクでないと考える提供者は、欧州委員会が構築しかつ管理する EU データベースに、自分自身を登録し、かつ AI システムに関する情報を登録する責任を負う。本規則の附属書におけるハイリスクのユースケースリストに記載されている AI システムを使用する前に、公的当局、公的事務所または公的機関であるハイリスク AI システムの導入者は、当該データベースに自分自身を登録し、かつ使用する予定のシステムを選択しなければならない。

他の導入者は、自発的にそのようにすることが認められなければならない。EU データベースのこのセクションは、無料で公衆がアクセスできるようにしなければならない。かつ、データベースにある情報は、容易なナビゲーションによって参照可能であり、容易に理解可能なものであり、機械により読み取り可能なものでなければならない。EU のデータベースは、また、ハイリスク AI システムの登録時に提出された関連情報、およびハイリスク AI システムが対応する本規則の附属書に定めるハイリスク AI システムのユースケースに関する関連情報を、公衆が発見できるようにするために、たとえば、キーワード検索を含む検索機能を提供するなど、ユーザーフレンドリーでなければならない。ハイリスク AI システムのあらゆる実質的な変更もまた、EU データベースに登録されなければならない。法執行行為、移民、亡命および出入国管理の分野におけるハイリスク AI システムについては、登録義務は、EU データベースの安全な非公開セクションにおいて履行されなければならない。安全な非公開セクションへのアクセスは、欧州委員会およびこのデータベースの国内セクションに関する市場監視当局に、厳密に制限される。重要インフラ分野におけるハイリスク AI システムは、国家レベルでのみ登録される。欧州委員会は、規則 (EU)2018/1725 に従って、EU データベースの管理責任者となる。いったん導入された EU データベースが完全に機能することを確保するため、データベースを創設する手続きは、欧州委員会による機能上の仕様の開発および独立した監査報告を含む。欧州委員会は、EU データベースの管理責任者としての任務を遂行する際、サイバーセキュリティに関するリスクを考慮しなければ

ならない。EU データベースを最大限に一般に利用可能としかつ活用するために、EU データベースは、それを通じて提供される情報を含め、指令(EU)2019/882 に定める要件を遵守しなければならない。

- (132) 自然人と交流し、またはコンテンツを生成することを目的とした一定の AI システムは、ハイリスクとみなされるかどうかにかかわらず、なりすましまたは欺瞞の特別のリスクをもたらし得る。したがって、一定の状況においては、これらのシステムの使用は、ハイリスク AI システムの要件と義務を害することなく、かつ法執行行為の特別な必要性を考慮することを目的とした的を絞った例外は別として、特別の透明性義務の対象としなければならない。特に、自然人は、使用状況および文脈を考慮し、合理的に十分な情報を持ち、注意深くかつ慎重な自然人の観点から、それが明らかな場合を除き、自然人が AI システムと交流していることを知らされなければならない。この義務を履行する際、その年齢または心身障害により脆弱なグループに属する自然人の特性は、AI システムがこれらのグループと交流することを目的としている範囲において、考慮されなければならない。さらに、自然人は、その生体データを処理することにより、これらの人の感情または意図を識別しもしくは推測することができ、または特定のカテゴリにこれらを割り当てることのできる AI システムにさらされた場合に、知らされなければならない。これらの特定のカテゴリは、性別、年齢、髪の色、目の色、入れ墨、個人的特徴、民族的出自、個人的な好みおよび個人的興味などの側面に関係し得る。これらの情報および通知は、心身障害者がアクセス可能なフォーマットで提供されなければならない。

(133) 各種の AI システムは、人間によって作成された真のコンテンツから区別することが人間にとってますます困難となる、大量の合成コンテンツを生成し得る。これらのシステムの幅広い利用可能性および向上しつつある性能は、情報処理エコシステムの完全性およびそれに対する信頼性に重大な影響を与え、これは誤情報や大規模な操作、不正、なりすまし、消費者詐欺の新たなリスクを生み出す。これらの影響、技術革新の急速なペース、ならびに情報の出所を明確にするための新たな方法および技術の必要性を考慮し、これらのシステムの提供者に、機械により読み取り可能なフォーマットによるマーキングができ、かつ出力が人間によってではなく AI システムによって生成されまたは操作されたことが検出できる、技術的ソリューションを組み込むことを要求することが適切である。このような技術および方法は、技術的にそれが実施可能な限り、十分に信頼でき、相互運用可能性があり、効果的かつ堅牢でなければならず、かつ、適宜、電子透かし、メタデータの識別、コンテンツの出所および真正性を証明するための暗号方式、ロギング方式、フィンガープリントまたはその他の技術など、利用可能な技術およびこれらの技術の組み合わせを考慮しなければならない。この義務を履行する際、提供者は、一般的に認められている最先端の技術に反映されているような、各種のコンテンツの特性および限界、ならびに当該分野における関連する技術および市場の発展も考慮しなければならない。これらの技術および方法は、コンテンツを生成する汎用 AI モデルを含む、AI システムのレベルまたは AI モデルのレベルにおいて実行することが可能であり、それにより AI システムの川下の提供者によるこの義務の履行を促進することになる。相応性に配慮し、このマーキングの義務は、主に標準的形式で実施支援機能を実行する AI システム、または導入者により提供される入力データまたはそのセマンティクスを大幅に変更しない AI システムには適用されないことが適切である。

- (134) AIシステムの提供者が使用する技術的ソリューションに加え、AIシステムを使用して、実在する人物、物、場所、主体、または出来事との著しい類似を示し、かつ人が本物または真実であるとの誤って捉え得る、画像、コンテンツ、音声、または動画(ディープフェイク)を、生成または操作する導入者は、AI出力の結果であることをラベリングし、したがって、その出所が人工的であることを明示して、コンテンツがAIにより作成されまたは操作されたことを、明確かつ合理的な方法により開示しなければならない。この透明性義務の遵守は、特にコンテンツが、明らかに創造的で、風刺的で、芸術的である作品またはプログラム、フィクションまたはそのような作品である場合、第三者の権利および自由のため適切なセーフガードの対象となることは別として、AIシステムの使用またはそれが生む出力の使用が、憲章により保証される表現の自由に対する権利、ならびに芸術および学術の自由に対する権利を妨げることを示すものとして、解釈されてはならない。これらの場合、本規則に基づくディープフェイクに適用される透明性義務は、作品の有用性および品質を完全に保持しつつ、その通常の利用および使用を含む、作品の表示または享受を妨げない適切な方法により、そのような生成または操作されたコンテンツの存在を公表することに限られる。さらにAIが生成または操作した文書に関し、AIが生成したコンテンツが人間によるレビューまたは編集管理のプロセスの対象となり、かつ自然人または法人がコンテンツの公表に対して編集責任を負うものでない限り、公共の利益に関する問題に関し公衆に情報提供する目的で、当該文書が公開される範囲で、同様の情報提供義務を検討することも適切である。
- (135) 透明性義務の義務的性質および完全な適用可能性を害することなく、欧州委員会は、また、EUレベルでの行動規範の作成を奨励し、かつ促進することができる。これは、AIにより生成されまたは操作されたコンテンツの検知およびラベリングに関する義務の効果的な実施を促進することを目的とし、必要に応じ、検証メカニズムに対するアクセスを可能とするための実務的方策、および公衆がAIにより生成されたコンテンツを効果的に認識できるよう、バリューチェーン全般にわたり他の行為者との協力を促進し、コンテンツを普及させまたはその正当性およびその出所を検証するための実務的方策を支援することを目的とすることを含む。

- (136) 一定の AI システムの出力が AI により生成されまたは操作されている事実を検出しおよび明示できるようにする目的で、本規則に基づきこれらの AI システムの提供者および導入者に課せられる義務は、規則(EU)2022/2065 の効果的な実施を促進するため特別な重要性を有する。これは、AI により生成されまたは操作されたコンテンツの拡散から生じ得るシステムック・リスク、特に、偽情報のバイアスによる、民主的プロセス、公の言論、および選挙プロセスに対する悪影響または予見可能なリスクを特定しかつ軽減するために、特に、非常に大規模なオンラインプラットフォームの提供者または非常に大規模なオンライン検索エンジンの提供者に課せられる義務に関して適用される。本規則に基づく AI システムによって生成されたコンテンツへのラベリング要件は、規則(EU)2022/2065 第 16 条第 1 項に基づきホスティングサービスプロバイダに課される受領した違法コンテンツに関する通知を処理する同規則第 16 条第 6 項に定める義務を害するものではなく、かつ問題のコンテンツの違法性に関する評価および決定に影響しない。この評価は、コンテンツの合法性を定めるルールを参照することによってのみ実施されなければならない。
- (137) 本規則の対象となる AI システムに適用される透明性義務の遵守は、AI システムの使用またはその出力の使用が、本規則または EU および加盟国のその他の立法に基づき合法であることを示すものとして解釈されるものではなく、かつ、EU 法または国内法に定める AI システムの導入者に対する他の透明性義務を害しない。
- (138) AI は、急速に発展している技術系統であり、責任あるイノベーション、ならびに適切なセーフガードおよび適切なリスク軽減措置の統合を確保しつつ、実験のための正規の監視の導入および安全かつ制御された場の導入を必要とする。イノベーションを促進し、時間の経過に耐え、かつトラブルに耐性のある法的枠組みを確保するため、加盟国は、革新的な AI システムの上市または他の方法によるサービス開始前に、厳格に規制されたコントロール下で、これらのシステムを開発しかつ試験を実施することを促進するため、その各国の所轄当局が、国内レベルで、少なくとも 1 つの正規 AI サンドボックスを設置することを確保しなければならない。加盟国は、また、既存の正規サンドボックスに参加することにより、または 1 つ以上の加盟国の管轄当局と共同でサンドボックスを設置することにより、この参加が、参加者である加盟国のために同程度の国内保証を提供する限り、この義務を充足することができる。正規 AI サンドボックスは、物理的形式、デジタル形式、またはハイブリッド形式で設置することができ、物理的な製品だけでなくデジタル製品にも適応し得る。また、設置する当局は、正規 AI サンドボックスが、財政的および人的リソースを含む、その機能を確保するための適切なリソースを保持することを確保しなければならない。

(139) 正規 AI サンドボックスは、革新的な AI システムが、本規則ならびにその他の EU 法および国内法の関連規定を遵守することの保証を目的とし、開発および商品化前の段階で、コントロールされた実験環境およびテスト環境を創設することにより、AI の分野におけるイノベーションを促進することを目的とする。さらに、正規 AI サンドボックスは、法的枠組みの将来における適応を目的とすることを含め、当局および企業のために規制された学習を促進するため、正規 AI サンドボックスに参加する当局との協力およびベストプラクティスの共有を支援するため、および、特にスタートアップを含む中小企業のために障壁を取り除くことにより市場へのアクセスを加速するため、イノベーターのために法的安全を高めることを目的とし、かつ管轄当局が、AI 使用の機会、新たなリスク、影響の監督および理解を高めることを目的とする。正規 AI サンドボックスは、EU 全体において広く利用可能でなければならず、スタートアップを含む中小企業にとってのアクセス可能性に、特に注意を払うことが適切である。正規 AI サンドボックスへの参加は、EU 域内において、AI を革新し、実験するために、かつ証拠となるデータに基づく規制された学習に貢献するために、提供者および潜在的提供者にとって、法的不安定を生む問題にフォーカスするものでなければならない。したがって、正規 AI サンドボックスにおける AI システムの監督は、そのシステムの上市またはサービス開始前の開発、訓練、テスト、検証を対象とし、および新たな適合性評価手続きを必要とする可能性のある実質的な変更の概念および実質的な変更の発生を対象としなければならない。これらの AI システムの開発およびテストの際に特定されたあらゆる重大なリスクは、適切な軽減措置をとる原因となり、かつ、それができない場合、開発およびテストのプロセスを停止する原因となる。

必要により、正規 AI サンドボックスを設置する各国の所轄当局は、基本的権利の保護を監督する当局を含む、他の関係当局と協力しなければならない。国内または欧州の標準化機関、認証機関、試験および実験施設、研究ラボおよび実験ラボ、欧州デジタルイノベーションハブならびに関係するステークホルダーおよび関係の市民社会など、AI エコシステムの他の行為者の参加を認めることができる。EU 域内全体における統一的な実施および規模の経済を確保するため、正規 AI 規制のサンドボックス設置のための共通ルール、およびサンドボックスの監督に関与する管轄当局間の協力の枠組みを確立することが適切である。本規則に基づき設置される正規 AI サンドボックスは、本規則以外に、法規の遵守を確保することを目的とする、他のサンドボックスの創設を認める他の法令を害しない。必要に応じ、これら他の正規サンドボックスに携わる関係する管轄当局は、AI システムが本規則に適合することを確保するためにも、これらのサンドボックスを使用する利点を考慮しなければならない。また、各国の所轄当局と正規 AI サンドボックスの対象者との間の合意を条件として、正規 AI サンドボックスの枠内において、監督されたリアルワールドテストを実施することも可能である。

(140) 本規則は、正規 AI サンドボックスの提供者および潜在的提供者が、規則(EU)2016/679 第 6 条第 4 項および第 9 条第 2 項(g)、ならびに規則(EU)2018/1725 第 5 条、第 6 条および第 10 条に従い、指令(EU) 2016/680 第 4 条第 2 項および第 10 条を害することなく、特定の条件の下でのみ、正規 AI サンドボックスの枠内において、公共の利益に関する一定の AI システムを開発するため、他の目的で収集された個人データを使用する法的根拠を構成する。規則(EU)2016/679 および規則 2018/1725 ならびに指令(EU)2016/680 に基づき、データ管理者のその他のあらゆる義務およびデータ主体のその他のあらゆる権利は、引き続き適用される。特に、本規則は、規則(EU)2016/679 第 22 条第 2 項(b)および規則(EU)2018/1725 第 24 条第 2 項(b)の意味において、法的根拠を構成するものではない。正規 AI サンドボックスの提供者および潜在的提供者は、適切なセーフガードを確保し、かつ当該サンドボックスにおける開発、テストおよび実験中に生じ得る安全、健康、および基本的権利に対する、特定されたあらゆる重大なリスクを適切に軽減するため、特にそのガイダンスに従いかつ迅速かつ誠実に行動することにより、管轄当局に協力しなければならない。

(141) 本規則の附属書に列挙されるハイリスク AI システムの開発プロセスおよび上市プロセスを加速するため、これらのシステムの提供者または潜在的提供者が、正規 AI サンドボックスに参加することなく、これらのシステムをリアルワールドテストの対象とするための特別な体制を享受できることも、重要である。しかし、そのような場合、これらのテストが自然人に及ぼし得る結果を考慮し、本規則は、提供者または潜在的提供者について、適切かつ十分な保証および条件を導入することを確保することが適切である。これらの保証は、インフォームドコンセントを求めることが AI システムのテストを妨げる法執行サービスに関する場合を除き、リアルワールドテストに参加するため、とりわけ、自然人側のインフォームドコンセントの請求を含むものでなければならない。本規則に基づきこれらのテストに参加に関する対象者の同意は、データ保護に関して適用される法に基づく個人データ処理に関するデータ主体の同意とは区別され、かつ、その同意を害するものではない。

また、リスクを最小限に減少させること、および管轄当局による監督を可能とすることも重要であり、したがって、潜在的提供者に対し、管轄の市場監視当局に提示されるリアルワールドテスト計画を保持することを要求すること、いくつかの限定的な例外は別として EU データベースの特定のセクションにテストを登録すること、テストが行われ得る期間に制限を定めること、および一定の脆弱なグループに属する人に追加的なセーフガードを要求すること、ならびに潜在的提供者と導入者の役割および責任を規定し、リアルワールドテストに参加する権限のある者による効果的な監督を定める書面による合意を要求することが重要である。さらに、データ保護に関する EU 法に基づくデータ主体として有する権利を害することなく、データ主体がテスト参加への同意を撤回した場合、AI システムの予測、提案または判断が、効果的に覆されかつ無視されることを確保するため、および個人データが保護されかつ削除されることを確保するため、追加的

なセーフガードを検討することが適切である。加えて、データ移転について、リアルワールドテストのために収集されかつ処理されたデータは、EU 法に基づき適切かつ適用可能なセーフガードが導入されている場合にのみ、特にデータ保護に関する EU 法に定める個人データ移転のための根拠に従って、第三国に移転されること、および、非個人データについては、特に、欧州議会および欧州理事会規則(EU)2022/868⁴²および(EU)2023/2854⁴³などの EU 法に従って、適切なセーフガードが導入されることが適切である。

- (142) AI が社会および環境に有益な結果をもたらすことを確保するため、加盟国は、心身障害者のアクセシビリティを向上させることを目的とする、社会経済的不平等に取り組むことを目的とする、または環境目標を達成することを目的とするような、AI に基づくソリューションなど、公的資金および EU の資金を含む十分なリソースを割り当てることにより、および必要に応じ、候補基準および選択基準が満たされる限りにおいて、これらの目的を追求する特別なプロジェクトを検討することにより、社会的および環境的に有益な結果を支援する AI ソリューションの研究開発を支援し、促進することが奨励される。これらのプロジェクトは、AI 開発者、不平等と非差別の分野、アクセシビリティの分野、消費者法の分野、環境法の分野およびデジタル法の分野に関する専門家ならびに研究者の間の、学際的な協力の原則に基づくものでなければならない。

⁴² 欧州データガバナンスに関する、および規則 (EU)2018/1724 を改正する 2022 年 5 月 30 日の欧州議会および欧州理事会規則(EU)2022/868 (データガバナンス規則) (OJ L 152, 3.6.2022, p.1)。

⁴³ データへの公平なアクセスおよびデータ使用についての統一ルールに関する、ならびに規則 (EU) 2017/2394 および指令 (EU) 2020/1828 を改正する 2023 年 12 月 13 日の欧州議会および欧州理事会規則 (EU) 2023/2854 (データ規則) (OJ L, 2023/2854、22.12.2023、ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>)。

(143) イノベーションを促進しかつ保護するため、AI システムの提供者または導入者であるスタートアップを含む中小企業の利益が、特に考慮されることが重要である。このため、加盟国は、特に、意識向上および情報伝達に関し、これらのオペレータを対象として、イニシアティブをとらなければならない。加盟国は、EU 域内にその本店または支店を有するスタートアップを含む中小企業に対し、正規 AI サンドボックスに対する優先的なアクセスを提供しなければならない。ただし、それらが候補条件および選択基準を満たすこと、および同じ条件および基準が満たされている限り、他の提供者や潜在的提供者がサンドボックスにアクセスすることを妨げないことを条件とする。加盟国は、それらにガイダンスを提供し、かつ本規則の実施に関するそれらの質問に回答することにより、その開発過程全般にわたり中小企業を支援するため、スタートアップを含む中小企業、導入者、その他のイノベーター、および必要に応じ、地方公共団体とのコミュニケーションのため、既存のコミュニケーションチャンネルを利用し、必要に応じ、新たなコミュニケーションチャンネルを導入する。必要に応じ、これらのチャンネルは、シナジーを創出するため、かつ、スタートアップを含む中小企業および導入者に対して提供されるガイダンスの一貫性を確保するために、協働するものでなければならない。さらに、加盟国は、標準化開発プロセスに対する、中小企業および他の関係するステークホルダーの参加を促進しなければならない。加えて、認証機関が適合性評価の手数料を決定する場合、スタートアップを含む中小企業である提供者の特別な利益およびニーズが考慮されなければならない。欧州委員会は、透明性のある協議を行い、スタートアップを含む中小企業のため、認証および適合性実施のコストを定期的に評価し、かつ、これらのコスト削減のため、加盟国と協力しなければならない。

例えば、義務的な文書に関する翻訳費用および当局と連絡に関する翻訳費用は、提供者およびその他のオペレータ、特に小規模なそれらの者にとっては、重大なコストとなり得る。加盟国は、場合により、提供者の関係文書およびオペレータとの連絡のため、加盟国が選択しおよび受容する言語の1つが、可能な限り多くの国境を越えた導入者により理解される言語であることを確保しなければならない。スタートアップを含む中小企業の特別のニーズに応えるため、欧州委員会は、AI 委員会の要請により、本規則の対象となる分野について、標準的なテンプレートを提供しなければならない。さらに、欧州委員会は、あらゆる提供者および導入者のために、本規則に関連して容易に利用できる情報を提供する単一の情報プラットフォームを開設すること、本規則から生じる義務に対する注意を高めるための適切なコミュニケーションキャンペーンを企画すること、AI システムに関連する公共調達手続きにおけるベストプラクティスの集約を評価しかつ促進することにより、加盟国が行う取組みを補完しなければならない。最近まで欧州委員会勧告 2003/361/EC⁴⁴ の附属書にいう小企業として認定されていた中企業は、これら新たな中企業が、本規則を適切に理解しかつ規定を遵守するために必要な法的リソースおよびトレーニングを欠いている可能性があるため、これらの支援措置へのアクセスが与えられなければならない。

⁴⁴ 零細企業および中小企業の定義に関する 2003 年 5 月 6 日欧州委員会勧告(OJ L 124, 20.5.2003, p. 36)。

- (144) イノベーションを促進しかつ保護するため、オンデマンドの AI プラットフォーム、ならびに EU または国レベルで欧州委員会および構成国によって設立された、デジタルヨーロッパプログラムおよびホライズンヨーロッパなど、欧州の関連するプログラムおよび関連する資金計画の全体が、必要に応じ、本規則の目的の実現に貢献するものでなければならない。
- (145) 市場における知識および専門知識の欠如に起因する実施に対するリスクを最小限に抑えるため、ならびに提供者、特にスタートアップを含む中小企業、および認証機関が本規則に基づきそれらに課される義務を遵守するよう促進するため、オンデマンドの AI プラットフォーム、欧州デジタルイノベーションハブ、ならびに EU レベルまたは国レベルで欧州委員会および加盟国によって設置された実験およびテスト施設は、本規則の実施に貢献するものでなければならない。オンデマンドの AI プラットフォーム、欧州デジタルイノベーションハブならびに実験およびテスト施設は、それぞれの任務および技能分野の枠内において、提供者および認証機関に対し、特に技術的および学術的支援を提供することができる。
- (146) さらに、規模が非常に小さい一部のオペレータを考慮し、イノベーションのコストに関する均衡を確保するため、零細企業が、最もコストのかかる義務の 1 つ、すなわち品質管理体制を導入する義務を、保護レベルおよびハイリスク AI システムに適用される要件の遵守の必要性に影響を与えることなく、これらの企業の管理上の負担およびコストを削減する簡易な方法により、充足することができるようにすることが適切である。欧州委員会は、零細企業が品質管理体制のどの要素を簡略なシステムにおいて遵守しなければならないかを明確にするため、ガイドラインを策定しなければならない。
- (147) 欧州委員会は、関係する EU 調和法に基づき設立または認証され、かつ問題の EU 調和法の対象となる製品または装置の適合性評価の枠内において任務を遂行する、機関、グループ、または研究所のために、試験および実験施設へのアクセスを、可能な範囲で促進することが適切である。これは、特に、規則(EU)2017/745 および(EU)2017/746 に基づく医療機器の分野における、専門家パネル、専門的研究所、およびリファレンスラボに関する場合である。

- (148) 本規則は、国家レベルで本規則の適用を調整しかつ支援するとともに、EU レベルで能力を強化すること、および AI 分野におけるステークホルダーをまとめることを可能とする、ガバナンスの枠組みを確立するものでなければならない。本規則の効果的な実施および施行には、EU レベルで中心的な専門知識を調整しおよび強化し得るガバナンスの枠組みが求められる。AI オフィスは、欧州委員会決定⁴⁵によって設立され、AI 分野における EU の専門知識を深めかつ能力を強化すること、および AI に関する EU 法の実施に貢献することを任務とする。加盟国は、EU レベルでの EU の専門知識および能力の発展を支援すること、およびデジタル単一市場の機能を強化することを目的とし、AI オフィスの任務達成を促進しなければならない。さらに、加盟国の代表者で構成される AI 委員会、学会をまとめることを目的とする学術パネル、ならびに EU レベルおよび国レベルで、本規則の実施のためにステークホルダーの協力を募ることを目的とする諮問フォーラムを設立することが適切である。EU の専門知識および能力の発展は、また、特に、EU レベルにおける他の法規の施行の文脈において構築されたストラクチャーとのシナジー、および Europa 共同企業、およびデジタルヨーロッパに関するプログラムの対象となる AI のテストおよび実験施設のような、EU レベルにおける関係するイニシアティブとのシナジーにより、既存のリソースおよび専門知識を利用することも含まれる。

⁴⁵ 欧州人工知能オフィスの設立に関する 2024 年 1 月 24 日の欧州委員会決定 (C/2024/ 390)。

(149) 本規則の円滑で効果的かつ統一の実施を促進するため、AI 委員会を創設することが適切である。AI 委員会は、AI エコシステムのさまざまな利益を考慮し、加盟国の代表者で構成されなければならない。AI 委員会は、多くの諮問業務を委ねられることになるが、そのなかには、本規則に定める要件についての施行に関する事項、技術仕様、または既存の規格を含む、本規則の実施に関連する事項についての意見、勧告、助言を発出すること、またはガイダンスへ貢献すること、および AI に関連する具体的な問題に関して、欧州委員会および加盟国ならびにその各国の所轄当局に対して助言を提供することがある。AI 委員会における加盟国の代表者の任命に、加盟国に対して一定の柔軟性を与えるため、これらの代表者は、国家レベルの調整を促進するため、および AI 委員会の任務達成に貢献するため、必要な能力および権限を有する公的団体に所属するあらゆる者になり得る。AI 委員会は、市場監視と認証機関のそれぞれに関係する問題について、市場監視当局と認定当局との間における協力および交流のためのプラットフォームを提供する任務を負う、2 つの常設サブグループを設置しなければならない。市場監視のための常設サブグループは、規則(EU)2019/1020 第 30 条にいう、本規則の管理協力グループ(ADCO)として行動しなければならない。当該規則第 33 条に従い、欧州委員会は、特に、市場監視当局間の緊急で特別な調整を必要とする本規則の側面を特定するため、市場の評価または研究を実施することにより、市場監視のための常設サブグループの活動を支援しなければならない。AI 委員会は、特定の問題を検討する目的で、必要に応じ、他の常設または臨時のサブグループを創設することができる。また、AI 委員会は、必要に応じ、関連する EU 法の文脈において活動する、管轄を有する機関、専門家グループ、およびネットワーク、特に、データ、デジタル製品およびデジタルサービスに関して適用される EU 法に基づき活動する者と協力しなければならない。

(150) 本規則の実施および適用に対するステークホルダーの関与を確保するため、アドバイザリー・フォーラムを設置し、AI 委員会および欧州委員会に助言する任務、および技術的な専門知識を提供する任務を課すことが適切である。商業的および非商業的なさまざまな利益を考慮し、商業的利益の範疇において、および、中小企業およびその他の企業に関し、ステークホルダーの多様かつ衡平な代表を確保するため、アドバイザリー・フォーラムは、特に、スタートアップ、中小企業、学界、社会的パートナーを含む市民社会、ならびに基本権エージェンシー、ENISA、欧州標準化委員会(CEN)、欧州電気標準化委員会(CENELEC)および欧州電気通信規格機構(ETSI)の分野の代表者で構成されなければならない。

- (151) 本規則の実施および施行、特に汎用 AI モデルに関する AI オフィスのモニタリング活動を支援するため、独立の専門家により構成される学術パネルを設置することが適切である。学術パネルを構成する独立の専門家は、AI 分野における最新の学術的または技術的な専門知識に基づき、選定されなければならない。専門家は、その任務を公平かつ客観的に遂行し、その任務および活動の遂行にあたって得た情報およびデータの秘密性を確保しなければならない。本規則の効果的な施行に必要な各国の能力を強化できるように、加盟国は、その法執行行為のため、学術パネルを構成する専門家の予備的人員の支援を要請することが可能でなければならない。
- (152) AI システムに関する適切な施行を支援するため、および加盟国の能力を強化するため、AI のテストのための EU の支援機構が創設され、かつ加盟国が利用できるようにしなければならない。
- (153) 加盟国は、本規則の適用および施行において、重要な役割を果たす。この点、各加盟国は、本規則の適用および施行を監督する各国の所轄当局として、少なくとも 1 つの認定当局、および少なくとも 1 つの市場監視当局を指定しなければならない。加盟国は、その具体的な国内の組織的特性およびニーズに応じ、種類を問わず、本規則にいう各国の所轄当局の任務を遂行する公的団体を指定することを決定することができる。加盟国側における組織の効率性を高め、かつ加盟国および EU レベルの公衆および他のカウンターパートとの単一の連絡窓口を設置するため、各加盟国は、単一の連絡窓口の役割を有する市場監視当局を指定しなければならない。
- (154) 各国の所轄当局は、その活動およびその任務の客観性の原則を保持するため、および本規則の適用および施行を確保するため、独立した、公平かつ偏りがない方法により、その権限を行使しなければならない。これらの当局のメンバーは、その職務と相容れないあらゆる行動を控え、かつ本規則に定める秘密保持のルールに従わなければならない。

(155) ハイリスク AI システムの提供者が、そのシステムならびに設計および開発プロセスを改善するため、ハイリスク AI システムの使用において獲得した経験を考慮に入れることができること、またはしかるべきときに可能な是正措置を講じることができることを確保するため、あらゆる提供者は市販後モニタリングシステムを導入する必要がある。必要に応じ、市販後モニタリングは、他のデバイスやソフトウェアを含む、他の AI システムとの相互作用の分析を含むものでなければならない。市販後モニタリングは、法執行機関である AI システムの導入者の機微取扱データを含むものであってはならない。このシステムは、上市後またはサービス開始後も「学習」し続ける AI システムから生じる潜在的リスクに、より効率的かつしかるべきときに対処できることを保証するためにも重要である。この文脈において、提供者は、AI システムの使用から生じるあらゆる重大インシデント、すなわち、死亡または健康への重大な侵害、重要インフラの管理および運用の重大かつ不可逆的な混乱、基本的権利の保護を目的とする EU 法に基づく義務の違反、または財産もしくは環境への重大な侵害をもたらすインシデントまたは誤作動を、管轄当局に報告するためのシステムを導入する責任を負う。

(156) EU 調和法の一部である本規則に定める要件および義務の適切かつ効果的な施行を確保するため、規則(EU)2019/1020 に定める製品の市場監視システムおよび適合性のシステムは完全に適用されなければならない。本規則に基づき指定された市場監視当局は、本規則および規則(EU)2019/1020 に定めるあらゆる執行権限を持ち、当局は、独立して、公平に、偏りのない方法によりその権限を行使し、その職務を遂行しなければならない。大部分の AI システムが本規則に基づく特定の要件および義務の対象でないとしても、市場監視当局は、それが本規則に従いリスクを示す場合、あらゆる AI システムに対し措置を講じることができる。本規則の適用範囲にある EU の機関、組織、部署および事務所の特別な性質により、欧州データ保護監督機関をそれらに関する管轄の市場監視当局として指定することが適切である。これは、加盟国による各国の所轄当局の指定を害するものではない。市場監視活動は、独立性が EU 法の要件を構成する場合、監督対象となる主体が独立して任務を遂行する権能に影響を与えない。

(157) 本規則は、平等の問題を扱う機関およびデータ保護当局を含む、基本的権利の保護に関する EU 法の適用を監督する当局または各国の管轄を有する公的機関の管轄、任務、権限および独立性を害しない。それらの権限により必要となる場合、これらの当局または各国の公的機関は、本規則に基づき作成されたあらゆる文書にアクセス可能でなければならない。健康、安全および基本的権利に対するリスクを示す AI システムに対して、適切かつしかるべきときに執行できることを保証するため、特別なセーフガード手続きが創設されなければならない。リスクを示すこれらの AI システムに適用される手続きは、リスクを示すハイリスク AI システム、本規則に定める禁止行為に違反して上市され、サービスが開始されまたは使用された禁止されたシステム、および本規則に定める透明性要件に違反し利用に供され、かつリスクを示す AI システムに、適用される。

(158) 金融サービスに関する EU 法は、金融サービスが AI システムを利用する場合を含め、これらのサービス提供の枠内において、規制される金融機関に適用される内部のガバナンスおよびリスク管理に関するルールおよび要件を含む。本規則および金融サービスに関する EU の法令に定める財務関連のルールおよび関連の要件から生じる義務の一貫性ある適用および施行を確保するため、これらの法令の監督および施行を任務とする管轄当局、特に欧州議会および欧州理事会規則(EU)No 575/2013⁴⁶および指令 2008/48/EC⁴⁷、2009/138/EC⁴⁸、2013/36/EU⁴⁹、2014/17/EU⁵⁰ および(EU)2016/97⁵¹という管轄当局は、加盟国がこれらの市場監視の任務を遂行する別の当局を指定するとの決定をしない限り、規制され監督下にある金融機関により提供または使用される AI システムに関し、市場監視活動を含む、本規則の実施を監督する目的で、それぞれの権限の範囲内で、管轄当局として指定されなければならない。

これらの管轄当局は、本規則および規則(EU)2019/1020 に基づき、金融サービスに関する EU 法に基づくその既存の監督メカニズムおよび手続きに、必要に応じ、統合し得る事後的市場監視

⁴⁶ 金融機関および投資会社に適用される財務健全性要件に関する、および規則 (EU)No 648/2012 を改正する 2013 年 6 月 26 日の欧州議会および欧州理事会規則(EU)No 575/2013 (OJ L 176, 27.6.2013, p.1)。

⁴⁷ 消費者信用契約に関する、および欧州理事会指令 87/102/EEC を廃止する 2008 年 4 月 23 日の欧州議会および欧州理事会指令 2008/48/EC (OJ L 133, 22.5.2008, p.66)。

⁴⁸ 保険および再保険事業へのアクセスおよびその遂行に関する 2009 年 11 月 25 日の欧州議会および欧州理事会指令 2009/138/EC (ソルベンシーII)(OJ L 335, 17.12.2009, p.1)。

⁴⁹ 金融機関事業へのアクセス、金融機関および投資会社の財務健全性の監督に関する、ならびに指令 2002/87/EC を改正し、および指令 2006/48/EC と 2006/49/EC を廃止する 2013 年 6 月 26 日の欧州議会および欧州理事会指令 2013/36/EU (OJ L 176, 27.6.2013, p.338)。

⁵⁰ 住宅用不動産の消費者信用契約に関する、ならびに指令 2008/48 / EC、2013/36 / EU および規則 (EU)No 1093/2010 を改正する 2014 年 2 月 4 日の欧州議会および欧州理事会指令 2014/17/EU (OJ L 60, 28.2.2014, p.34)。

⁵¹ 保険販売に関する 2016 年 1 月 20 日の欧州議会および欧州理事会指令(EU)2016/97(OJ L 26, 2.2.2016, p.19)。

活動を実施する権限を含む、本規則の要件および義務を遵守させるために必要なあらゆる権限を有する。当局が、本規則に基づく市場監視当局として行動する場合、EU 理事会規則(EU)No 1024/2013⁵²によって導入された単一監督メカニズムに参加する指令 2013/36/EU により規制される金融機関の監督責任者である国内当局は、上記規則に定める財務健全性監督業務など、欧州中央銀行(ECB)の財務健全性監督業務のために利益となり得るその市場監視活動の枠内において特定されたあらゆる情報を、遅滞なく、欧州中央銀行に報告することを想定することが適切である。

本規則と指令 2013/36/EU により規制される金融機関に対して適用されるルールとの間の一貫性をより強化するため、リスク管理、市販後モニタリング、および文書化に関し、提供者の一定の手続的義務を、指令 2013/36/EU に基づく既存の義務および手続きに統合することも適切である。重複を避けるため、提供者の品質管理体制、およびハイリスク AI システムの導入者に課せられる監視義務に関し、それに関する規定が指令 2013/36/EU により規制される金融機関に適用される範囲で、限定的な例外も考慮しなければならない。同じ体制は、指令 2009/138/EC の対象となる保険会社、再保険会社および保険持株会社、ならびに指令(EU)2016/97 の対象となる保険仲介業者、ならびに金融分野における一貫性および平等な取扱いを確保するため、金融サービスに関係する EU 法の関係規定に基づき導入された内部のガバナンス、取決めまたはプロセスに関する要件の対象となるその他の種類の金融機関に適用されなければならない。

- (159) 本規則の附属書に列挙される生体認証の分野におけるハイリスク AI システムの各市場監視当局は、これらのシステムが法執行行為、移民、亡命および出入国管理、または司法行政および民主的プロセスに関する目的で用いられる範囲内において、少なくとも、処理されるあらゆる個人データおよびその任務を遂行するために必要なあらゆる情報にアクセスする権限を含む、調査および是正措置における効果的な権限を有するものでなければならない。市場監視当局は、完全に独立して、その権限を行使し得るものでなければならない。本規則に基づく機微取扱データに対するそのアクセスのあらゆる制限は、指令(EU)2016/680 によりそれに与えられた権限を害しない。本規則に基づく各国のデータ保護当局に対するデータ開示に関するいかなる除外も、本規則の適用範囲を超えて、これらの当局の現在または将来の権限に影響を与えない。

⁵² 金融機関の財務健全性監督に関する政策について欧州中央銀行に特定の任務を与える 2013 年 10 月 15 日の欧州理事会規則(EU)No 1024/2013 (OJ L 287, 29.10.2013, p.63)。

- (160) 市場監視当局および欧州委員会は、2 か国以上の加盟国において重大なリスクを示すことが判明したハイリスク AI システムの特定の種類に関し、本規則に関する法の遵守を促進し、不遵守を特定し、意識を向上させ、かつガイダンスを提供することを目的として、市場監視当局が実施する、または市場監視当局が欧州委員会と共同で実施する、共同調査を含む、共同の活動を提案することができる。法の遵守を促進するための共同の活動は、規則(EU)2019/1020 第 9 条に従って、実施されなければならない。AI オフィスは、共同調査のため、調整の支援を提供する。
- (161) 汎用 AI モデル上に構築される AI システムに関し、EU レベルおよび国家レベルで、責任および管轄を明確にする必要がある。AI システムが汎用 AI モデルに基づくものであり、かつモデルおよびシステムが同一の提供者により提供されている場合、管轄の重複を避けるため、監督は、この目的のため、規則(EU)2019/1020 にいう市場監視当局の権限を有する AI オフィスを通じ、EU レベルで行われる。それ以外のすべての場合、各国の市場監視当局は、引き続き AI システムの監督に責任を負う。ただし、ハイリスクに分類される少なくとも 1 つの使用のため、導入者が直接使用できる汎用 AI システムについては、市場監視当局は、適合性評価を実施するため、かつ、しかるべく AI 委員会およびその他の市場監視当局に通知するため、AI オフィスと協力する。さらに、すべての市場監視当局は、ハイリスク AI システム上に構築されている汎用 AI モデルに関係する一定の情報にアクセスできないとの理由により、市場監視当局がハイリスク AI システムに関する調査を完了することができない場合、AI オフィスに支援を要請することができなければならない。そのような場合、規則(EU)2019/1020 第 VI 章に定める国境を越えるケースについての共助に関する手続きが準用されなければならない。
- (162) EU の集約された専門知識および EU レベルにおけるシナジーを最大限に活用するため、汎用 AI モデルの提供者に課せられる義務の遵守を監督および施行する権限は、欧州委員会の管轄に属する。AI オフィスは、汎用 AI モデルに関し、本規則の効果的な実施を監督するため、必要なすべての措置をとることができる。AI オフィスは、汎用 AI モデルの提供者に課せられるルール違反の可能性を、そのモニタリング活動の結果に従って自発的に、または本規則に定める条件に従って市場監視当局の要請により、調査することができる。AI オフィスの効果的なモニタリングに貢献するため、AI オフィスは、川下の提供者に対し、汎用 AI モデルおよび汎用 AI システムの提供者に関するルール違反の可能性に関する苦情を申し立てる手段を提供する。

(163) 汎用 AI モデルのガバナンスシステムを補完するため、学術パネルは AI オフィスのモニタリング活動を支援し、場合により、AI オフィスに対し、調査などのフォローアップ措置のきっかけとなる適格な警告を発することができる。これは、汎用 AI モデルが EU レベルで具体的かつ特定可能なリスクを示すことを学術パネルが疑う理由がある場合である。さらに、汎用 AI モデルが、システミック・リスクを示す汎用 AI モデルとして分類され得る基準を満たすことを学術パネルが疑う理由がある場合である。学術パネルはこれらの任務の遂行に必要な情報を得るため、欧州委員会に対し、提供者に文書または情報を提出することを要求するよう請求できる仕組みが必要である。

(164) AI オフィスは、本規則に定める汎用 AI モデルの提供者に課せられる義務の効果的な実施および義務の遵守を監督するため、必要な措置を講じることができる。AI オフィスは、文書および情報を求めること、評価を実施すること、汎用 AI モデルの提供者が措置をとることを求めることなど、本規則に基づき AI オフィスに与えられる権限に従い、違反の可能性を調査することができる。評価実施の際、独立した専門知識を活用する目的で、AI オフィスは、その名で評価を実施するため、独立の専門家の支援を求めることができる。義務の遵守は、とりわけ、適切な措置を講じることが、請求により強制し得るものでなければならない。これにはシステミック・リスクが特定された場合のリスク軽減措置、ならびに市場において利用に供されるモデルの制限、およびモデルの撤去またはそのリコールを含む。セーフガードとして、本規則に定める手続的権利に加えて必要な場合、汎用 AI モデルの提供者は、規則(EU)2019/1020 第 18 条に定める手続的権利を享受し、本規則で定めるより具体的な手続的権利を害することなく、この規定が準用される。

(165) 本規則の要件を遵守して、ハイリスク AI システム以外の AI システムを開発することは、EU において倫理的かつ信頼できる AI のより大幅な採用につながり得る。ハイリスクではない AI システムの提供者は、行動規範を策定するよう奨励される。これには、ハイリスク AI システムに適用される義務的要件の一部または全部の自発的な適用の促進を目的とし、システムの意図目的および問題となるより低いリスクに適応し、かつモデルやデータカードなど、利用可能な技術的ソリューションおよび産業分野のベストプラクティスを考慮する、関連するガバナンス体制を含む。また、ハイリスクかどうかを問わず、あらゆる AI システムおよび AI モデルの提供者、および必要に応じその導入者は、追加的要件を自発的にかたちで適用することも奨励される。追加的要件は、たとえば、信頼できる AI のための EU の倫理ガイドラインの要素、環境の持続可能性、AI リテラシーに関する措置、および AI システムの非排他的かつ多様な設計および開発に関するものであり、AI システムの設計および開発に、脆弱な人、障害者のアクセシビリティ、必要に応じて、関係するステークホルダーの関与、たとえば、企業および市民社会の組織、学界、研究機関、労働組合、消費者保護団体などのステークホルダーが参加すること、およびジェンダーバランスを含む開発チームの多様性に配慮することを含む。自発的な行動規範が実効性を持つためには、明確な目標、およびこれらの目標の達成度を測ることができる重要業績評価指標(KPI)に基づくことが必要である。また、行動規範は、必要に応じ、企業や市民社会の組織、学界、研究機関、労働組合、消費者保護団体など、関係するステークホルダーの関与により、非排他的な方法で策定されなければならない。欧州委員会は、特に、データへのアクセスインフラ、および異なる種類のデータのセマンティックで技術的な相互運用性など、AI 開発のための国境を越えたデータ交換を妨げる技術的障壁を取り払うことを促進するため、分野別のものを含む、イニシアティブを策定することができる。

(166) 本規則に基づくハイリスクではない製品であり、したがってハイリスク AI システムについて定められた要件を遵守する必要がない製品に関連する AI システムは、上市時またはサービス開始時に、とにかく安全であることが重要である。この目的に寄与するため、欧州議会および欧州理事会規則(EU)2023/988 が⁵³、セーフティネットとして適用される。

⁵³ 製品の安全性全般に関する、ならびに欧州議会および欧州理事会規則 (EU) No 1025/2012 および欧州議会および欧州理事会指令 (EU) 2020/1828 を改正し、欧州議会および欧州理事会指令 2001/95/EC および理事会指令 87/357/EEC を廃止する 2023 年 5 月 10 日の欧州議会および欧州理事会規則 (EU) 2023/988 (OJ L 135, 23.5.2023, p. 1)。

- (167) EU レベルおよび国レベルで管轄当局の建設的で信頼のおける協力を確保するため、本規則の適用に関与するすべての当事者は、EU 法および国内法に従い、その任務遂行の枠内で得た情報およびデータの機密性を保持しなければならない。当事者は、特に、知的財産権、秘密情報および営業秘密、本規則の効果的な実施、公共の安全および国家安全保障上の利益、刑事手続きおよび行政手続きの完全性、ならびに国家機密情報の完全性を保護するような方法で、その任務および活動を遂行しなければならない。
- (168) 本規則の遵守は、制裁およびその他の執行措置を課すことにより、強制され得る。加盟国は、本規則の規定が確実に実施されるよう、必要なあらゆる措置を講じ、かつ、特にこれらの規定に違反した場合における効果的で、相応で、かつ抑止的な制裁を、一事不再理の原則に従って規定する。本規則の違反の場合に適用される行政罰の強化および統一を図るため、一定の具体的違反行為に対する制裁金の定めに上限金額を定めることが適切である。制裁金の額の算定のため、加盟国は、個別の事案において、特に違反の性質、重大性、期間、およびその結果、ならびに提供者の規模、とくに、特に提供者がスタートアップを含む中小企業である場合を考慮するなど、具体的状況に関連するあらゆる事情を考慮しなければならない。欧州データ保護監督機関は、本規則の対象となる EU の機関、組織、部署および事務所に対し、罰金を科す権限を有する。
- (169) 本規則に基づき汎用 AI モデルの提供者に課せられる義務の遵守は、とりわけ、制裁金によって強制され得る。このため、比例原則に従った適切な時効期間を条件として、本規則に基づき欧州委員会が要求した措置に従わなかったことを含め、これらの義務の違反に対して、適切なレベルの制裁金もまた定められなければならない。本規則に基づき欧州委員会が下したあらゆる決定は、欧州連合機能条約に従って欧州司法裁判所による審理対象となり、これには欧州連合機能条約第 261 条の適用による制裁に関する欧州司法裁判所の完全な管轄を含む。
- (170) EU 法および国内法は、AI システムの使用により、その権利および自由が害され得る自然人および法人に対する効果的な救済措置を、既に規定している。これらの救済措置を害することなく、本規則の違反があったと考える理由を有するあらゆる自然人または法人は、関係する市場監視当局に対し、苦情を申し立てる権利を有する。

- (171) 関係者は、導入者の決定が、主に、本規則の適用範囲内にある一定のハイリスク AI システムの出力に基づくものであり、かつこの決定が法的効果を生じるものであるか、またはこれらの関係者が、その健康、安全または基本的権利に悪影響を及ぼすと考える方法で、これらの者に同様に重大な影響を与える場合に、説明を受ける権利を有する。この説明は、明確かつ意味のあるもので、かつ関係者がその権利を行使し得る根拠を構成するものでなければならない。説明を受ける権利は、例外または制限が EU 法または国内法に基づく AI システムの使用に対して適用されるものではなく、かつこの権利が、EU 法によりまだ定めがない範囲内においてのみ、適用される。
- (172) 本規則に対する違反の通報者として行動する者は、EU 法に基づき保護される。したがって、欧州議会および欧州理事会指令(EU)2019/1937⁵⁴は、本規則の違反の通報、およびそのような違反を通報する者の保護に対して適用される。
- (173) 規制の枠組みが必要に応じて適応できることを保証するため、欧州連合機能条約第 290 条に従って法を採択する権限は、AI システムがハイリスクであると見なされない条件、ハイリスク AI システムのリスト、技術文書に関する規定、EU 適合宣言書の内容、適合性評価手続きに関する規定、品質管理体制の評価および技術文書の評価に基づく適合性評価手続きが適用されるハイリスク AI システムを定める規定、システムック・リスクを示す汎用 AI モデルの分類に関するルールにおいて、ベンチマークと指標を補完することを含む、閾値、ベンチマークおよび指標、システムック・リスクを示す汎用 AI モデルの指定基準、汎用 AI モデルの提供者向けの技術文書、および汎用 AI モデルの提供者のための透明性に関する情報の各条件の修正が可能となるよう、欧州委員会に委任される。欧州委員会は、専門家レベルを含む、準備作業において適切な協議を実施すること、およびこれらの協議は、「より良い立法」に関する 2016 年 4 月 13 日の機関間協定⁵⁵に定める原則に従って実施されることが、特に重要である。特に、委任法令の法案作成への平等な参加を確保するため、欧州議会および欧州理事会は、すべての文書を加盟国の専門家と同時に受領する。それらの専門家は、委任法令の法案作成に参加する欧州委員会の専門家グループの会合に当然にアクセスできる。

⁵⁴ EU 法違反を通報する者の保護に関する 2019 年 10 月 23 日の欧州議会および欧州理事会指令 (EU)2019/1937(OJ L 305, 26.11.2019, p.17)。

⁵⁵ OJ L 123, 12.5.2016, p1

(174) 急速な技術の進展、および本規則を効果的に適用するために必要な技術的な専門知識を考慮し、欧州委員会は、遅くとも【本規則の発効日から 5 年の】年月日までに、およびその後は 4 年ごとに、本規則を評価および再検討し、欧州議会および欧州理事会に報告する。さらに、本規則の適用範囲に対する影響を考慮し、欧州委員会は、ハイリスク AI システムのリストおよび禁止行為のリストを、年に一度修正する必要性の評価を実施する。加えて、遅くとも【本規則の発効日から 4 年の】年月日までに、およびその後は 4 年ごとに、欧州委員会は、本規則の附属書記載のハイリスクとなる分野のリスト項目、透明性義務の対象となる AI システム、監視およびガバナンス体制の有効性、ならびに追加的措置または追加的行為の必要性を含む、汎用 AI モデルの良好な開発に関する標準化デリヴァブルの成果の進捗状況について、修正の必要性を評価し、かつ欧州議会および欧州理事会に報告する。最後に、遅くとも【本規則の発効日から 4 年の】年月日までに、およびその後は 3 年ごとに、欧州委員会は、ハイリスク AI システム以外の AI システムの場合において、ハイリスク AI システムに対して定める要件の適用、および必要に応じ、当該 AI システムに対するその他の追加的要件の適用を促進することを目的とする自主的な行動規範の影響および有効性を評価する。

(175) 本規則を実施する統一的条件を保証するために、欧州委員会に実施の権限を委ねることが適切である。これらの権限は、欧州議会および欧州理事会規則(EU)No 182/2011⁵⁶に従って行使される。

⁵⁶ 加盟国による欧州委員会の実施権限の行使の管理体制に関するルールおよび一般原則を規定する 2011 年 2 月 16 日の欧州議会および欧州理事会規則(EU)No 182/2011 (OJ L 55, 28.2.2011, p.13)。

- (176) 本規則の目的（すなわち、EU 域内における AI システムの悪影響から民主主義、法の支配および環境保護を含む、健康、安全、および欧州連合基本権憲章に記されている基本的権利のハイレベルな保護を保証しつつ、かつイノベーションを支援しつつ、域内市場の機能を向上させること、および人間を中心とする信頼できる AI の採用を促進すること）が、加盟国によっては十分に達成し得ないが、活動の規模または効果を理由に、EU レベルでよりよく達成し得るのであれば、EU は、欧州連合条約第 5 条に記されている補完性の原則に従って、措置を講じることができる。同条に定める比例性の原則に従い、本規則は、この目的を達成するために必要な範囲を超えるものではない。
- (177) 法的安全を確保し、オペレータが適切な対応期間を有することを確保し、かつ AI システムの使用の継続性を確保しつつ、市場のあらゆる混乱を回避するため、本規則は、その一般的な適用日より前に上市され、またはサービスが開始されたハイリスク AI システムに対し、この日以降、これらのシステムの設計または意図的に重要な変更が加えられる場合にのみ、適用されることが適切である。この点に関し、重要な変更の概念は、本規則に基づきハイリスク AI システムに関してのみ使用される実質的な変更の概念と本質的に実質的に同等と理解されることを明確にすることが適切である。例外的に、かつ公衆に対する説明責任に照らし、本規則の附属書に列挙される法令に定める大規模な IT システムの構成要素である AI システムのオペレータおよび、公的機関により使用されることを目的とするハイリスク AI システムのオペレータは、それぞれ、現在から 2030 年末まで、かつ遅くとも年月日[本規則の発効日から 6 年後]までに、本規則の要件を遵守するための必要な措置を講じなければならない。
- (178) ハイリスク AI システムの提供者は、移行期間において、本規則の関係する義務の自発的な遵守開始が奨励される。

(179) 本規則は、[本規則の発効日から2年の]年月日から適用される。しかし、AIの一定の使用に関連する容認できないリスクを考慮すると、本規則の禁止事項および一般規定は、[本規則の発効日から6か月の]年月日から、既に適用される。これらの禁止事項の完全な効果は、本規則のガバナンスの実施および施行により生ずるとしても、容認できないリスクを考慮し、たとえば民法などの他の手続き上で効果を有するように、禁止事項の適用を早めることが重要である。さらに、ガバナンスおよび適合性評価体制に関連するインフラは、[本規則の発効日から2年の]年月日より前に運用され、したがって、認証機関およびガバナンス構造に関する規定は、[本規則の発効日から12か月の]年月日から適用されなければならない。技術の進歩の急速性および汎用AIモデルの採用の急速性を考慮すると、汎用AIモデルの提供者に課せられる義務は、[本規則の発効日から12か月の]年月日から適用されるべきである。行動規範は、提供者が遅れることなくその遵守を証明できるように、[本規則の発効日から9か月の]年月日までに準備しなければならない。AIオフィスは、技術の進展に照らし、分類のルールおよび手続きが最新であることを確保しなければならない。さらに、加盟国は、制裁金を含む、制裁に関するルールを定め、かつ欧州委員会に通知し、かつ本規則の適用日までに、それらが適切かつ効果的に実施されるよう確保しなければならない。したがって、制裁に関する規定は、[本規則の発効日から12か月の]年月日から適用されなければならない。

(180) 欧州データ保護監督機関および欧州データ保護委員会は、規則(EU)2018/1725 第42条第1項および第2項に従って諮問され、2021年6月18日に共同の意見を述べた。

本規則を採択した：