

ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第9巻第3号（通巻第57号・2024年8月）

法と情報研究会 編

本号目次

[資料]

夏井高人 規則(EU)2024/1689(人工知能法) [前文の参考訳]

1~130頁

規則(EU) 2024/1689(人工知能法) [前文の参考訳]

2024 年 8 月 31 日
明治大学法学部教授
夏井 高人

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJL, 2024/1689, 12.7.2024) のテキスト(英語版)に基づき、その和訳を試みた。

原文のテキストを入手できるサイトの URL は、下記のとおりである。

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
[2024 年 7 月 12 日確認]

— 解 説 —

1. 規則(EU) 2024/1689(人工知能法)について

規則(EU) 2024/1689 の案(COM/2021/206 final)は、2021 年 4 月 22 日に欧州委員会から提案され、必要な審議が重ねられ(2021.0106 COD)、審議の過程で合意された正文案に関して非常に多数の誤記訂正が行われた上で 2024 年 5 月 21 日(第 3 読会)において理事会の承認を受けた後、2024 年 6 月 13 日に欧州議会の代表及び理事会の代表による署名が行われた。

その後、約 1 か月間にわたるミスタイプ等の原文修正作業を経た後、2024 年 7 月 12 日、EU 官報上で規則(EU) 2024/1689 として公示された。

これらの手続きにより、規則(EU) 2024/1689 が欧州連合の規則(Regulation)として内部的にも外部的にも成立した。

規則(EU) 2024/1689 の略称は、その表題に明確に示されているとおり、「人工知能法(Artificial Intelligence Act)」である。EU 官報上で公示されている正規の略称であり、EU 官報上で公示されている以上、この略称の指定部分も法規の一部なので、規則(EU) 2024/1689 を示すものとしては、この「人工知能法」以外の略称は認められないが、前文と条文の中では「Artificial Intelligence」の略称として「AI」を用いているので、「AI 法」という略称は認められていると解される。

規則(EU) 2024/1689 の略称としては、現時点では使用が認められない語としては、例えば、「AI 規制法」や「AI 規則」などがある。「AI 規制法」との訳は、意味的にみても完全に誤訳である。

規則(EU) 2024/1689(以下「AI 法」という。)は、同法第 113 条により、2024 年 8 月 1 日に発効した。

AI 法は、以下のとおりに適用される。

第 I 章及び第 II 章の条項は、2025 年 2 月 2 日から。

第 III 章第 4 節、第 V 章、第 VII 章及び(第 101 条を除く)第 XII 章の各条項並びに第 78 条は、2025 年 8 月 2 日から。

第 6 条第 1 項及び対応する各義務は、2027 年 8 月 2 日から。

(第 6 条第 1 項及び対応する各義務、第 4 節を除く)第 III 章、第 IV 章、第 VI 章、第 VIII 章、(第 78 条を除く)第 IX 章、第 X 章、第 XI 章、第 XIII 章の各条項並びに第 101 条は、2024 年 8 月 2 日から。

AI 法の立法提案の理由等は、提案書(COM(2021)206 final)の中で詳述されている。

COM(2021)206 final

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

[2024 年 8 月 20 日確認]

AI 法の内容を正確に理解するためには、この提案書(COM(2021)206 final)だけではなく、AI 法の前文の中で参照されている幾つかの関連資料等を精読・理解する必要がある。

そのような必須資料の中で、例えば、ハイレベル専門家グループ(HLEG)によって作成された『信頼できる AI に関する倫理指針(Ethics guidelines for trustworthy AI)』は、下記のところにある。

Ethics guidelines for trustworthy AI

<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

[2024 年 2 月 14 日確認]

AI 法の前文(77)の中で示されている「デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則(a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements)」は、AI 法が公示された時点ではまだ審議中であり、未採択の規則案(COM/2022/454 final)のことを指す。

規則案(COM/2022/454 final)は、AI 法と密接な関連性をもつものなので、AI 法の理解と適正な解釈を得るため、同規則案の採択の後には無論のこと、規則案の段階から内容理解に努めるべきものである。規則案(COM/2022/454 final)の正文は、下記のところにある。

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454>

[2024 年 8 月 19 日確認]

AI 法の原文には誤記と疑われる箇所が複数残存している。それゆえ、今後、EU 官報上で公示される正誤表(Corrigendum)により、原文の修正が追加される可能性がある。

2. 参考訳作成における基本方針

この参考訳においては、AI 法の前文(recital)、条文(articles)及び別紙(annex)を訳出した。ただし、諸般の事情に鑑み、法と情報雑誌上で分割して公表することにした。

この参考訳においては対訳方式を採用することにした。ただし、原文を表示することが無意味な部分(特に脚注内)に関しては、原文または訳文の表示を省略した。

この参考訳は、あくまでも AI 法の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は、現時点における研究成果を反映するものである。将来、更に研究を深めた結果として修正すべき部分を発見したときは、その時点において、改訂版等を作成すべきかどうかを検討する。

この参考訳は、法と情報雑誌 6 巻 5 号上で人工知能規則案(COM2021/206 final)の参考訳を公表した後に更に調査研究を進めた上での現時点における研究成果を反映している。そのため、この参考訳においては、人工知能規則案の参考訳における訳文及び訳語とは異なっている箇所が多数ある。誤解や誤訳などの箇所は、再検討した上で全て改めた。

参考訳の訳出に際しては原則として直訳とすることとしたが、直訳のままでは日本語になりにくい箇所に関しては、やむを得ず意識した。

この参考訳に訳注はない。参考訳中にある脚注は、全て原注である。

この参考訳は AI 法の注釈書ではないので、それらの箇所の全てを指摘することは避け、必要に応じて合理的に解釈した上で訳文を作成することにした。

訳出の理由に関する個別の説明がなければ当該箇所の訳出の理由がわかりにくいと想定される箇所に関しては、必要に応じて、「参考訳作成において留意した事項」の中で説明を加えることとした。

原文中にある誤記と疑われる箇所に関しては、**赤色字**で示すこととした。この原文中の誤記と疑われる箇所は、形式的なミスという意味で誤記であるものと意味的な誤りを含むことになるために誤記であるものの両者を含む。

ただし、原文中に存在する誤記と疑われる箇所の全てが**赤色字**で表示されているという趣旨ではない。判断を保留した箇所が存在する。

読みやすさを重視し、条文中の号(point)の表記を一部省略した。例えば、「point(a)」は「第(a)号」であるが、「第」と「号」を省略し、「(a)」と表記することにした。

この参考訳は、Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

Critical infrastructures

「critical infrastructures」は、一般に、「重要インフラ」と訳されている。私もこれまではそのように訳してきた。しかし、EU の法制全体を見渡した場合、「critical infrastructures」と「important infrastructures」とを分けて理解する必要が高い。

そこで、この参考訳を含め、今後は、「critical infrastructures」を「不可欠なインフラ」または「不可欠インフラ」と訳し、「important infrastructures」を「重要なインフラ」または「重要インフラ」と訳すことにした。

なお、日本国の関連法制における「重要インフラ」との概念は、基本的には、EU の関連法制における「critical infrastructures」の概念に対応するものなので、この分野における日本国の関連立法中の法概念及び語彙と EU 法の関連立法中の法概念及び語彙とは一致していない。

General-purpose AI system, general-purpose AI Model

「general-purpose AI system」は、「汎用 AI システム」と訳されることが多い。実際、異なる様々な目的のために使用可能なシステムは存在するので、その意味で「汎用」かもしれない。

しかし、一般的な日本語の語彙としての「汎用性」をもたない「general-purpose AI system」も存在し、特殊な目的または専門的な目的のためには使用できないという意味で汎用性の要素を欠くシステムも存在する。それゆえ、この場合における「general-purpose」を「汎用」と訳すと、(消費者保護や製品の安全性の観点からも)問題が生じ得ることを否定できない。

EU 法の中における「general」という語または概念の代表的な用例と比較して検討してみると、例えば、General Data Protection Regulation (GDPR)における「general」は、「汎用」という意味をもたない。

GDPR に定める適用範囲に従い、EU の機関における個人データ処理、構成国の警察活動における個人データ処理、PNR と関連する個人データ処理に関しては、規則(EU) 2018/1725、指令(EU) 2016/680、指令(EU) 2016/681 のような別の法令が適用され、また、国防や国家安全保障等と関連する分野に対してはそもそも GDPR の適用がない。

そのため、GDPR における「general」とは、これら別の法令が適用される分野及びそもそも GDPR の適用のない分野を控除した「残余の分野」という意味しかもたず、「汎用」という意味を全くもたない。

それにもかかわらず、あえて「General Data Protection Regulation」を「汎用データ保護規則」と訳すとすれば、そのような訳は、誰が考えても明らかに誤訳である。

そして、AI 法の中では、EU の AI 法が全ての AI システム及び AI モデルに適用されるのではなく、例えば、医療機器規則(EU) 2017/745、体外診断用医療機器規則(EU) 2017/746 及び機械規則(EU) 2023/1230 のような別の法令が適用され、AI 法が適用されることのない分野が存在することを明示で認めている。

つまり、AI 法における「general-purpose」は、AI 法の適用範囲から判断しても「汎用」ではなく、それらの別の法令が適用される分野を控除した「残余の分野」という意味しかもたない。

そこで、この参考訳においては、とりあえず、「general-purpose AI system」を「一般目的 AI システム」と訳し、また、同様の理由により、「general-purpose AI Model」を「一般目的 AI モデル」と訳すことにした。

なお、直訳を貫き、かつ、長くなることを厭わないときは、「general-purpose AI system」を「一般的な目的な AI システム」と訳し、また、同様の理由により、「general-purpose AI Model」を「一般的な目的の AI モデル」と訳し得る。

Supervised learning, unsupervised learning

人工知能技術(AI 技術)の分野では、一般に、「supervised learning」は「教師あり学習」と訳され、「unsupervised learning」は「教師なし学習」と訳されている。ここで想定されている「教師」とは、生徒の自主的な学習や自力による成長を想定しない機械的な訓練の指導者のことだと思われるが、現在ではそのような教師像に対しては否定的な見解が多い。加えて、技術開発の現場で実際に行われているのは都合の悪いデータセットまたはモデルの除去・整形と一定のバイアスを付与するための調整である。人間の教師が人間の生徒に対して同じことを実行すると、その行為は、「洗脳」または「思想統制」もしくは「思想強制」として理解される。日本国憲法及び国連の児童の権利条約の下において、そのような行為は禁止される。それゆえ、ここで「教師」という語を用いるのは適切ではない。人間の「教師」の役割がそのようなものと誤解される危険性があるからである。

一般に、教師は、調教師ではない。より正確に言えば、動物の調教師の場合であっても、調教の対象とする動物の個性・特徴・能力を 100%把握し、当該動物から信頼されるような態様でその動物の能力が最大限発揮されるように調教を実施するのではなければ、所期の効果をあげることなどできない。「教師あり学習」との訳における「教師」とは、教師ではなく、独裁主義の国における軍事教練のようなものを想定しているのではないかと疑われる。そのような場合の軍事教練の指導者・指揮官は、絶対服従の上官ではあり得ても、教師ではない。

以上の諸点を考慮に入れた上で、この参考訳においては、「supervised learning」を「監督あり学習」と訳し、「unsupervised learning」を「監督なし学習」と訳すことにした。

Notified body

「notified body」は、職務権限のある国内機関(competent national authorities)によって指定を受け、かつ、欧州委員会に対して通知された適合性評価組織である。

「notified body」は、構成国の行政機関の一種であり得るけれども、民間の特殊な能力をもつ評価組織または監査組織が「notified body」となることが想定されている。ただし、企業の会計監査や情報セキュリティ上の監査とはかなり異なり、得意分野とする AI 技術別に区分された指定が行われることが想定されている。

現時点においては、全ての種類の AI 技術及びその応用製品と応用サービスに関して、技術上の要求事項及び法律上の要件と義務の充足の有無を単一の監査法人等が完全に審査・評価・判断することは、ほぼ不可能である。少なくとも、現時点の日本国内において、AI 法の中で示された必須の要件を充足する業務遂行能力と中立性と公平性を満たす民間組織は、1 つも存在しないし、今後もビジネスとして成立する見込みはほとんどない。それゆえ、日本国においては、民間企業ではなく、国の厳格な管理の下にある特別の研究組織等が個人情報保護委員会と協力しながら「notified body」としての役割を果たさざるを得ないのであるかと考えられる。

以上を踏まえた上で、「notified body」は、直訳では「被通知組織」または「通知された組織」と訳すことになる。

しかし、このような訳語を用いる場合、「notified body」に期待されている極めて重要な任務と機能を反映するものではないという意味で適切な訳語ではない。

そこで、この参考訳においては、その意味を反映させるため、「notified body」を「指定組織」と意識することにした。

Work-related contractual relationships

「work-related contractual relationships」として表現される場合の「contractual relationships」は、古典的な使用者と労働者との間の契約関係を規律する雇用契約だけではなく、雇用とは異なる形態による労務の提供や仕事の完成などの給付を契約内容とする請負契約、委任契約、準委任契約のような契約を基礎とする契約関係も含めた表現である。

ただし、ある仕事と関係するという特徴をもつ契約類型であることから「work-related」と表現していると解される。

そこで、この参考訳においては、「work-related contractual relationships」を「仕事関連の契約関係」と訳すことにした。ここでいう「仕事関連」とは、雇用契約の場合を含むが、雇用契約に限定されないという趣旨の表現である。

Democratic processes

「democratic processes」とは、通常は、民主主義という政治思想(政治哲学)を基礎として国家機能の一部とされている選挙制度(election system)により、大統領や首相のような現実の統治担当者を選任するプロセスのことを指す。

ところが、EU の構成国の中には王制を維持している国家があり、元は構成国だった英国も王制を採用している。王制の国家における選挙制度は、共和制国家における選挙制度とは政治学上の位置づけが異なるものであり得る。しかし、どのような国家体制を選択するかは、当該国家の国家主権の本質部分(=どのような集団またはどのような一族が権力を握る資格をもつか?)であり、(実力説を基礎として考えると)国家権力の正当性根拠そのものでもあるので、基本的に他国からの干渉が許されない。また、国家主権の本質部分であるがゆえに、その点に関する他国からの干渉は、直ちに外患を組成するのであり、そのことのゆえに国家間の戦争(武力紛争)へと発展することがある。

それゆえ、AI 法を含め、EU の主要法令の中では、大統領や首相のような現実の統治担当者を選任するプロセスのことを示すために、端的に「election」とは表現せず、「democratic processes」と表現するのが通例となっている。

以上のことを踏まえた上で、この参考訳においては、「democratic processes」を「民主的な過程」と訳すことにした。

Regulatory sandboxes

EU の構成国には様々なタイプの「regulatory sandboxes」が存在し、かつ、適用される制度の相違により、当該サンドボックスの特性や機能が異なっているため、画一的な訳語をあてはめることが許されない語の一つとなっている。

「regulatory sandboxes」の訳語としては、一般に、「規制サンドボックス」が使用されることが多い。しかし、例えば、あるシステムが「適法であること」は、当然の一般要件であって規制法令による義務ではないので(日本国の民法第 1 条及び第 90 条参照)、「適法であること」を適用除外することのできる実験場のような場所は、特定の規制法令の条項を根拠とする「規制」のサンドボックスではないことになる。

AI 法の立法理由を述べる提案書(COM(2021) 206 final)の説明書(Explanatory Memorandum)の 525 は、「第 V 款は、技術革新フレンドリで、将来耐性があり、かつ、混乱に抗する回復力のある法的枠組みをつくり出すという目的のために貢献する。その目的のために、第 V 款は、職務権限のある国内機関が、regulatory sandboxes を設置し、かつ、統治、監督及び法的責任の面における基本的な枠組みを定めることを推進する。AI regulatory sandboxes は、職務権限のある機関との間で合意した試験計画を基礎とする限定された期間内、革新的な技術を試験するための管理された環境を構築する」と述べている。AI 法の中では前文(138)及び前文(139)にその解説がある。

つまり、AI 法における「regulatory sandboxes」は、「特定の規制法令の条項を根拠とする規制を免除する」という機能だけをもつものではなく、個々の事業者と構成国の関係当局との間の個々の合意に従い、閉鎖環境または実世界環境において、(合意に基づいて特定の法令の特定の条項を適用除外とすることのできる)様々な恩典や免除などを含み得る実験を実行することのできる機能をもつ場のことを意味する。それゆえ、AI 法における「regulatory sandboxes」を「規制サンドボックス」と訳すと、AI 法において「regulatory sandboxes」を設けた趣旨を没却しかねない。

そもそも「sandboxes」は、語それ自体として、「免除された場」というニュアンスをもっているので、「規制サンドボックス」では二重に訳していることともなりかねない。

他方において、AI 法における「regulatory sandboxes」の根拠法令が AI 法すなわち規則(EU) 2024/1689 にあることを前提にして考えてみると、「regulatory sandboxes」という表現は、「規則(EU) 2024/1689 を根拠とするサンドボックス」というニュアンスをもつ語としても理解可能である。

ちなみに、EU の法形式の一種である規則(Regulation)を「規制」と訳出している各種文献(報告書、論文等)が存在するが、完全な誤訳である。「regulatory sandboxes」を「規制サンドボックス」と訳している例では、そのような傾向が顕著にあると言える。諸般の事情を考慮し、この点に関する具体的な例示は避けることにする。

以上の諸点を考慮に入れた上で、この参考訳においては、AI 法案の参考訳の時点で採用した「regulatory sandboxes」の訳語である「法定サンドボックス」を変更し、「法制サンドボックス」を用いることにした。ただし、「regulatory sandboxes」に関し、より良い訳語が存在するときは、それによるべきである。

Statement of conformity, declaration of conformity

AI 法第 47 条所定の「EU declaration of conformity」において用いられている「declaration of conformity」の概念と規則(EU) 2019/881 の第 52 条所定の「EU statement of conformity」において用いられている「statement of conformity」の概念とは、規則(EU) 2019/881 の前文(81)を読んで理解できる範囲内では同一の内容をもつ概念であり、表現が異なるだけであると解される。

規則(EU) 2019/881 の参考訳・改訂版においては「statement of conformity」を「適合性宣言書」と訳した。AI 法における「declaration of conformity」もまた、意味的に全く同じ内容をもつ概念を指すものなので、「適合性宣言書」と訳すことにした。

'Real-time'

AI 法の中には「'real-time'」と「real-time」が混在して使用されている。しかし、最終的に採択された版の正文の定義条項(第 3 条第 42 号)では「'real-time'」ではなく「real-time」が使用されている。そのことから、この定義条項で使用されている表現が正規の表現となると解される。その結果、前文及び条文中に残存している「'real-time'」との表現は全て(修正漏れによる)誤記の一種であることになる。

この参考訳においては、以上のように解した上で、合理的に訳出することにした。

4. 関連参考訳等

人工知能規則案 (COM/2021/206 final) の参考訳は、法と情報雑誌 6 巻 5 号 320～562 頁にある。

デジタルの権利及び基本原則に関する欧州宣言 (2023/C 23/01) の参考訳は、法と情報雑誌 9 巻 1 号 200～229 頁にある。

規則(EU)2022/2065 (デジタルサービス法) の参考訳は、法と情報雑誌 8 巻 2 号 1～299 頁にある。デジタル単一市場著作権指令(EU)2019/790 の参考訳は、法と情報雑誌 7 巻 1 号 1～113 頁にある。

製造物責任に関する理事会指令 85/374/EEC の参考訳は、法と情報雑誌 2 巻 10 号 278～291 頁にある。AI 法的責任指令案の参考訳は、法と情報雑誌 8 巻 1 号 1～80 頁にある。先端デジタル技術の法的責任に関する欧州委員会スタッフ作業文書 SWD (2018) 137 final の参考訳は、法と情報雑誌 3 巻 9 号 233～268 頁にある。

規則(EU) 2016/679 (一般データ保護規則) の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU) 2018/1725 の参考訳は、法と情報雑誌 4 巻 1 号 1～81 頁にある。指令(EU) 2016/680 の参考訳は、法と情報雑誌 2 巻 1 号 41～140 頁にある。指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。

規則(EU) 2019/881 (Cybersecurity Act) の参考訳・改訂版は、法と情報雑誌 4 巻 8 号 16～86 頁にある。理事会枠組み決定 2002/584/JHA の参考訳は、法と情報雑誌 4 巻 5 号 185～213 頁にある。

指令(EU)2022/2557 の参考訳は、法と情報雑誌 8 巻 4 号 207～303 頁にある。

この参考訳には、新保史生氏 (慶應義塾大学総合政策学部教授) との間における意見交換の結果等が反映されている。

ただし、原文の読解及び内容の解釈、関連法令の法解釈を含め、この参考訳の文責は、全て夏井高人にある。

この参考訳の校正等に関し、唐亀侑久氏 (株式会社ラック) の助力を得た。

人工知能に関する整合化された諸規定を定め, 規則(EC)No 300/2008, 規則(EU)No 167/2013, 規則(EU)No 168/2013, 規則(EU) 2018/858, 規則(EU) 2018/1139 及び規則(EU) 2019/2144 並びに指令 2014/90/EU, 指令(EU) 2016/797 及び指令(EU) 2020/1828 を改正する 欧州議会及び理事会の 2024 年 6 月 13 日の規則(EU)2024/1689(人工知能法)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(EEA に適用される正文)

(Text with EEA relevance)

欧州議会及び欧州連合の理事会は、
欧州連合の機能に関する条約、とりわけ、その第 16 条及び第 114 条に鑑み、
欧州委員会からの提案に鑑み、
立法案を国内議会に送付した後、
欧州経済社会委員会の意見書に鑑み¹、
欧州中央銀行の意見書に鑑み²、
地域委員会の意見書に鑑み³、
通常の立法手続に従って審議し⁴、

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,
Having regard to the opinion of the European Central Bank ⁽²⁾,
Having regard to the opinion of the Committee of the Regions ⁽³⁾,
Acting in accordance with the ordinary legislative procedure ⁽⁴⁾,

Whereas:

¹ OJ C 517, 22.12.2021, p. 56.

² OJ C 115, 11.3.2022, p. 5.

³ OJ C 97, 28.2.2022, p. 60.

⁴ 欧州議会の 2024 年 3 月 13 日付け立場表明書(官報未搭載)及び理事会の 2024 年 5 月 21 日の決定。
Position of the European Parliament of 13 March 2024 (not yet published in the Official Journal) and decision of the Council of 21 May 2024.

- (1) この規則の目的は、とりわけ、欧州連合内における人工知能システム(AI システム)の開発、それを市場に置くこと、サービスに供すること及びその利用に関し、欧州連合の価値に従って統一的な法的枠組みを定めることにより、域内市場の稼働を向上させること、健康、安全、並びに、民主主義、法の支配及び環境保護を含め欧州連合基本権憲章(「憲章」)に掲げられている基本的な権利の高いレベルの保護を確保しつつ、人間中心でありかつ信頼できる人工知能(AI)の導入を促進すること、欧州連合内における AI システムの危険な影響に抗して防御すること、及び、技術革新を支えることにある。この規則は、AI ベースの物品及びサービスの国境を越える支障のない移動を確保し、そして、この規則によって明示で認められている場合を除き、AI システムの開発、マーケティング及び利用に対して構成国が制限を加えることを防止することを確保する。

The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the ‘Charter’), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

- (2) この規則は、技術革新と雇用を加速し、かつ、欧州連合を、信頼できる AI の導入におけるリーダーにしつつ、自然人、事業者、民主主義の保護及び法の支配並びに環境保護を促進している憲章に掲げられている欧州連合の価値に従って適用されるべきである。

This Regulation should be applied in accordance with the values of the Union enshrined as in the Charter, facilitating the protection of natural persons, undertakings, democracy, the rule of law and environmental protection, while boosting innovation and employment and making the Union a leader in the uptake of trustworthy AI.

- (3) AI システムは、国境を越える場合を含め、非常に多様な経済部門及び社会の多くの部分において容易に設置され得るのであり、かつ、欧州連合全域において容易に流通し得る。ある構成国は、AI が信頼できかつ安全であること、そして、基本的な権利上の義務に従って開発及び利用されることを確保するための国内規定の採択を既に模索している。諸国内規定に格差があることは、域内市場の断片化を導き得るのであり、また、AI システムを開発、輸入または利用する運用者にとっての法的確実性を低下させ得る。それゆえ、運用者に関する統一的な義務を定めることによって、及び、欧州連合の機能に関する条約(TFEU)の第 114 条を基礎として、域内市場全体にわたる公共の利益及び個人の権利という優越的な根拠に基づく統一的な保護を保障することによって、域内市場内における AI システム及び関連製品と関連サービスの支障のない流通、技術革新、設置及び導入を妨げる多様性は排除されるべきものとしつつ、信頼できる AI を達成するため、欧州連合全域にわたる一貫性がありかつ高いレベルの保護が確保されるべきである。法執行の目的のためのリモートの生体要素識別のための AI システムの利用の制限、法執行の目的のための自然人のリスク評価のための AI

システムの利用の制限, 及び, 法執行の目的のための生体要素類型への振分けの AI システムの利用の制限と関係する個人データの処理と関連する個人の保護に関する細目規定がこの規則が含んでいる範囲内において, それらの細目規定が関係する範囲内で, この規則が TFEU の第 16 条を基礎とすることが適切である。それらの細目規定及び TFEU の第 16 条への依拠に照らし, 欧州データ保護委員会から意見聴取することが適切である。

AI systems can be easily deployed in a large variety of sectors of the economy and many parts of society, including across borders, and can easily circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that AI is trustworthy and safe and is developed and used in accordance with fundamental rights obligations. Diverging national rules may lead to the fragmentation of the internal market and may decrease legal certainty for operators that develop, import or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured in order to achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market should be prevented by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, of the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and of the use of AI systems of biometric categorisation for the purpose of law enforcement, it is appropriate to base this Regulation, in so far as those specific rules are concerned, on Article 16 TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

- (4) AI は, 産業界及び社会活動の全範囲にわたる幅広い経済, 環境及び社会の受益に貢献する急速に進化しつつある技術ファミリーである。予測を向上させること, 運用と資源配分を最適化すること, そして, 個人と組織にとって利用可能なデジタルソリューションを個別化することによって, AI の利用は, 事業者に対して鍵となる競争上の優位を提供でき, また, 例えば, 医療, 農業, 食品の安全, 教育と訓練, メディア, スポーツ, 文化, インフラの運営管理, エネルギー, 輸送及び物流, 公共サービス, 保安, 法務, 資源とエネルギーの効率性, 環境の監視, 生物多様性とエコシステムの保護と回復, そして, 気候変動の緩和と気候変動への適応において, 社会上及び環境上の有益な成果を支え得る。

AI is a fast evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial s, for example in healthcare, agriculture, food safety, education and training, media, sports, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, the conservation and restoration of biodiversity and ecosystems and climate change mitigation and adaptation.

- (5) それと同時に、AI の個々の応用、利用及び技術上の発展のレベルと関連する状況の相違に応じて、AI は、欧州連合法によって保護されている公共の利益及び基本的な権利に対するリスクを生成し、また、それらに対する危険を生じさせ得る。そのような危険は、物的、心理的、社会的または経済的な危険を含め、有形または無形であり得る。

At the same time, depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm.

- (6) AI が社会に対してもち得る大きな影響及び信頼を構築する必要性に鑑み、AI 及びその法制枠組みに関しては、欧州連合条約 (TEU) の第 2 条に掲げられている欧州連合の価値、諸条約に掲げられている基本的な権利及び自由に従って、並びに、TEU の第 6 条により、憲章に従って構築されることが不可欠である。前提条件として、AI は、人間中心の技術であるべきである。AI は、人間の良好な状態を向上させることを究極の狙いとしてもつ、人々のためのツールとして奉仕すべきである。

Given the major impact that AI can have on society and the need to build trust, it is vital for AI and its regulatory framework to be developed in accordance with Union values as enshrined in Article 2 of the Treaty on European Union (TEU), the fundamental rights and freedoms enshrined in the Treaties and, pursuant to Article 6 TEU, the Charter. As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.

- (7) 健康、安全及び基本的な権利と関連する公共の利益の一貫性がありかつ高いレベルの保護を確保するため、高リスク AI システムに関する共通の規定が設けられるべきである。それらの規定は、憲章と一貫性があり、非差別であり、かつ、欧州連合の国際取引上の確約に沿うものであるべきである。それらの諸規定は、デジタル 10 年のためのデジタルの権利及び基本原則に関する欧州宣言並びに人工知能に関するハイレベル専門家グループの信頼できる AI に関する倫理指針 (AIHLEG) も考慮に入れるべきである。

In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, common rules for high-risk AI systems should be established. Those rules should be consistent with the Charter, non-discriminatory and in line with the Union's international trade commitments. They should also take into account the European Declaration on Digital Rights and Principles for the Digital Decade and the Ethics guidelines for trustworthy AI of the High-Level Expert Group on Artificial Intelligence (AIHLEG).

- (8) それゆえ、欧州連合法によって認められかつ保護されている民主主義、法の支配及び環境保護を含め、健康と安全のような公共の利益の高いレベルの保護と基本的な権利の保護とに同時に適合する域内市場における AI の開発、利用及び導入を育成するため、AI に関する整合化された規定を定める欧州連合の法的枠組みが必要である。その目的を達成するため、一定の AI システムを市場に置くこと、サービスに供すること及びその利用を規律する規定が定められるべきであり、そして、域内市場の円滑な稼働を確保する規定、並びに、それらのシステムが物品及びサービスの支障のな

い移動の原則から受益できるようにする規定が定められるべきである。それらの諸規定は、基本的な権利の保護において明確かつ堅牢であり、新たな革新的なソリューションを支えるのであり、欧州連合の価値に沿って AI システムをつくり出す公的関与者及び民間関与者の欧州のエコシステムを実現し、かつ、欧州連合の全領域にまたがるデジタル変革の可能性を解放つものであるべきである。それらの諸規定を定めることにより、また、スタートアップを含め、小企業及び中企業(SMEs)に特に焦点を当てた技術革新支援措置を定めることにより、この規則は、欧州理事会⁵によって述べられたような AI に対する人間中心の欧州のアプローチを促進するという目的及び安全で、信頼できかつ倫理的な AI の開発におけるグローバルなリーダーになるという目的を支え、また、この規則は、欧州議会から特に要請されたような倫理上の基本原則の保護を確保する。

A Union legal framework laying down harmonised rules on AI is therefore needed to foster the development, use and uptake of AI in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, including democracy, the rule of law and environmental protection as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market, the putting into service and the use of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. Those rules should be clear and robust in protecting fundamental rights, supportive of new innovative solutions, enabling a European ecosystem of public and private actors creating AI systems in line with Union values and unlocking the potential of the digital transformation across all regions of the Union. By laying down those rules as well as measures in support of innovation with a particular focus on small and medium enterprises (SMEs), including startups, this Regulation supports the objective of promoting the European human-centric approach to AI and being a global leader in the development of secure, trustworthy and ethical AI as stated by the European Council⁵, and it ensures the protection of ethical principles, as specifically requested by the European Parliament⁶.

- (9) 高リスク AI システムを市場に置くこと、サービスに供すること及びその利用に適用可能な整合化された規定は、欧州議会及び理事会の規則(EC) No 765/2008⁷、欧州議会及び理事会の決定 No 768/2008/EC⁸並びに欧州議会及び理事会の規則(EU) 2019/1020⁹(新たな立法枠組み)との一貫性を

⁵ 欧州理事会、欧州理事会の特別会合(2020年10月1日及び2日)―決議, EUCO 13/20, 2020, p. 6.

European Council, Special meeting of the European Council (1 and 2 October 2020) — Conclusions, EUCO 13/20, 2020, p. 6.

⁶ 人工知能、産業用ロボット及び関連技術の倫理上の側面の枠組みに関する欧州議会の 2020 年 10 月 20 日の決議及び欧州委員会への勧告 2020/2012(INL).

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

⁷ 承認の要件を定め、規則(EEC) No 339/93を廃止する欧州議会及び理事会の 2008 年 7 月 9 日の規則(EC) No 765/2008(OJ L218, 13.8.2008, p. 30).

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L218, 13.8.2008, p. 30).

⁸ 製品のマーケティングのための共通枠組みに関する、及び、理事会決定 93/465/EEC を廃止する欧州議会及び理事会の 2008 年 7 月 9 日の決定 No 768/2008/EC(OJ L218, 13.8.2008, p. 82).

Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L218, 13.8.2008, p. 82).

保って定められるべきである。この規則の中で定められた整合化された規定は、諸部門を横断して適用されるべきであり、かつ、新たな立法枠組みに沿って、とりわけ、データ保護、消費者保護、基本的な権利、雇用及び労働者保護並びに製品の安全性に関する現行の欧州連合法であって、それらの欧州連合法に対してこの規則が補完的となっているものを妨げてはならない。その結果として、理事会指令 85/374/EEC⁹⁾によりあり得る損害の弁償と関連するものを含め、当該の者に対して AI システムが負の影響をもつかもしれない消費者及びそれ以外の者のためにそのような欧州連合法によって定められている全ての権利及び救済は、影響を受けることなく、かつ、全面的に適用可能なままである。それゆえ、更に、雇用及び労働者保護の文脈において、この規則は、職場における健康と安全及び使用者と労働者との間の関係を含め、社会政策に関する欧州連合法に対して、及び、雇用及び労働条件と関係する欧州連合法に従う国内労働法に対して影響を与えてはならない。この規則は、ストライキをし、または、構成国内の個別の産業関連制度に包摂されているストライキ以外の行動をとる権利もしくは自由、並びに、集団的な協約を交渉し、締結し及び実行し、または、国内法に従って集団的な行動をとる権利を含め、当該構成国内において及び欧州連合レベルで認められた基本的な権利の行使に対しても影響を与えてはならない。この規則は、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及び理事会の指令の中で定められるプラットフォーム労働における労働条件の改善を狙いとする条項に対して影響を与えてはならない。それに加えて、この規則は、AI システムの透明性、技術文書及び記録の保管との関連を含め、個別の要件及び義務を設けることにより、そのような既存の権利及び救済の実効性を強化することを狙いとしている。更に、AI の価値連鎖に関与する様々な運用者に対してこの規則の下において課される義務は、そのような法律がこの規則の適用範囲外にある場合、または、この規則によって求められる公共の利益上の目的以外の正当な公共の利益上の目的を求める場合には、一定の AI システムの利用を制限する効果をもつ欧州連合法に従う国内法を妨げることなく適用されるべきである。例えば、国内労働法並びにデジタル環境における児童の権利に関する UNCRC 一般見解第 25 号(2021 年)を考慮に入れている未成年者すなわち 18 歳未満の者の保護に関する法律は、当該法律が AI システムに特化されておらず、かつ、それ以外の正当な公共の利益上の目的を求めるものである限り、この規則による影響を受けてはならない。

Harmonised rules applicable to the placing on the market, the putting into service and the use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council⁽⁷⁾ Decision No 768/2008/EC of the European Parliament and of the Council⁽⁸⁾ and Regulation (EU) 2019/1020 of the European Parliament and of the Council⁽⁹⁾ (New Legislative Framework). The harmonised rules laid down in this

⁹ 製品の市場監視及び法令遵守に関する、並びに、指令 2004/42/EC、規則(EC) No 765/2008 及び規則(EU) No 305/2011 を改正する欧州議会及び理事会の 2019 年 6 月 20 日の規則(EU) 2019/1020(OJ L 169, 25.6.2019, p. 1).

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

¹⁰ 欠陥のある製品の法的責任に関する構成国の法律、規則及び行政条項の近似化に関する 1985 年 7 月 25 日の理事会指令 85/374/EEC(OJ L 210, 7.8.1985, p. 29).

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).

Regulation should apply across sectors and, in line with the New Legislative Framework, should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, and protection of workers, and product safety, to which this Regulation is complementary. As a consequence, all rights and remedies provided for by such Union law to consumers, and other persons on whom AI systems may have a negative impact, including as regards the compensation of possible damages pursuant to Council Directive 85/374/EEC⁽¹⁰⁾ remain unaffected and fully applicable. Furthermore, in the context of employment and protection of workers, this Regulation should therefore not affect Union law on social policy and national labour law, in compliance with Union law, concerning employment and working conditions, including health and safety at work and the relationship between employers and workers. This Regulation should also not affect the exercise of fundamental rights as recognised in the Member States and at Union level, including the right or freedom to strike or to take other action covered by the specific industrial relations systems in Member States as well as the right to negotiate, to conclude and enforce collective agreements or to take collective action in accordance with national law. This Regulation should not affect the provisions aiming to improve working conditions in platform work laid down in a Directive of the European Parliament and of the Council on improving working conditions in platform work. Moreover, this Regulation aims to strengthen the effectiveness of such existing rights and remedies by establishing specific requirements and obligations, including in respect of the transparency, technical documentation and record-keeping of AI systems. Furthermore, the obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to national law, in compliance with Union law, having the effect of limiting the use of certain AI systems where such law falls outside the scope of this Regulation or pursues legitimate public interest objectives other than those pursued by this Regulation. For example, national labour law and law on the protection of minors, namely persons below the age of 18, taking into account the UNCRC General Comment No 25 (2021) on children's rights in relation to the digital environment, insofar as they are not specific to AI systems and pursue other legitimate public interest objectives, should not be affected by this Regulation.

- (10) 個人データの保護の基本的な権利は、とりわけ、欧州議会及び理事会の規則(EU) 2016/679¹¹及び規則(EU) 2018/1725¹²並びに欧州議会及び理事会の指令(EU) 2016/680¹³によって安全確保されている。

¹¹ 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679(一般データ保護規則)(OJ L 119, 4.5.2016, p. 1).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

¹² 欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護に関する並びにそのデータの支障のない移動に関する、並びに、規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

¹³ 犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行の目的のための職務権限のある機関による個人データの処理と関連する自然人の保護に関する、並びに、理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680 (OJ L 119, 4.5.2016, p. 89).

欧州議会及び理事会の指令 2002/58/EC¹⁴は、端末機器内に個人データ及び非個人データを記録保存するための条件または端末機器からアクセスするための条件を提供するという方法による場合を含め、私生活及び通信の秘密を付加的に保護する。それらの欧州連合の法行為は、データセットが個人データ及び非個人データの混合を包含している場合を含め、持続的かつ責任あるデータ処理のための基礎を提供する。この規則は、それらの法律文書の遵守を監視する職務権限のある独立の監督機関の職務及び権限を含め、個人データの処理を規律する現行の欧州連合法の適用に対して影響を与えることを求めていない。この規則は、AI システムの設計、開発または利用が個人データの処理を包摂する範囲内において、個人データの保護に関する欧州連合法または国内法から派生するデータの管理者または処理者としての当該の者の役割内における AI システムの提供者及び設置者の義務に対しても影響を与えない。プロファイリングを含め、自動化された個人の判定のみの場合と関連する権利を含め、そのような欧州連合法によってデータ主体に対して与えられた全ての権利及び保障をデータ主体が享受し続けることを明確にすることも適切である。AI システムを市場に置くこと、サービスに供すること及びその利用に関してこの規則の下において設けられる整合化された規定は、個人データの保護に関する欧州連合法の下において保障されたデータ主体の権利及びそれ以外の救済並びにこれ以外の基本的な権利の実効的な実装を促進し、かつ、その行使を実現すべきである。

The fundamental right to the protection of personal data is safeguarded in particular by Regulations (EU) 2016/679⁽¹¹⁾ and (EU) 2018/1725⁽¹²⁾ of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council⁽¹³⁾. Directive 2002/58/EC of the European Parliament and of the Council⁽¹⁴⁾ additionally protects private life and the confidentiality of communications, including by way of providing conditions for any storing of personal and non-personal data in, and access from, terminal equipment. Those Union legal acts provide the basis for sustainable and responsible data processing, including where data sets include a mix of personal and non-personal data. This Regulation does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. It also does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors stemming from Union or national law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data. It is also appropriate to clarify that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated **individual** decision-making, including profiling. Harmonised rules for the placing on the market, the putting into service and the use of AI systems established under this Regulation should facilitate the effective

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

¹⁴ 電子通信部門における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC(プライバシー及び電子通信に関する指令) (OJ L 201, 31.7.2002, p. 37).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

implementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protection of personal data and of other fundamental rights.

- (11) この規則は、欧州議会及び理事会の規則(EU) 2022/2065¹⁵⁾に定める中間介在サービスプロバイダの法的責任に関する条項を妨げてはならない。

This Regulation should be without prejudice to the provisions regarding the liability of providers of intermediary services as set out in Regulation (EU) 2022/2065 of the European Parliament and of the Council⁽¹⁵⁾.

- (12) この規則における「AI システム」の概念は、明確に定義されるべきであり、かつ、この分野における急速な技術開発に合わせるための柔軟性を提供しつつ、法的確実性を確保し、かつ、国際的な収斂と広範な受容を容易にするため、AI に関して作業している国際組織の作業と緊密に揃えられるべきである。それに加え、その定義は、より単純な在来のソフトウェアシステムまたはプログラミングのアプローチから AI システムを区別する AI システムの鍵となる特徴を基礎とすべきであり、また、業務を自動的に実行するために自然人のみによって定義されたルールを基礎とするシステムを包摂してはならない。AI システムの鍵となる特徴は、AI システムの推論するための能力である。この推論するための能力とは、予測、内容、推奨または判定のような、物理環境または仮想環境に対して影響を与え得る出力を得るプロセスのことを指し、また、入力またはデータからモデルもしくはアルゴリズムまたはその両者を導出するための AI システムの能力のことを指す。AI システムを構築しながら推論を実現する技法は、一定の目的をどのようにして達成するかをデータから学習する機械学習のアプローチ、並びに、コード化された知識または解決されるべきタスクのシンボリックな表現から推論する論理ベースのアプローチ及び知識ベースのアプローチを含む。AI システムの推論するための能力は、学習、推論またはモデリングを実現することにより、基礎的なデータ処理を超越する。「機械ベース」という用語は、機械装置上で AI システムが走っていることを指す。明示または黙示の目的の参照は、明示で定義された目的または黙示の目的に従って AI システムが運用可能であることを強調している。AI システムの目的は、個々の過程においては、当該 AI システムの所期の目的とは異なり得る。AI システムによって生成される出力は AI システムによって遂行される異なる機能を反映し、かつ、予測、内容、推奨または判定を含むので、この規則の目的のために、環境は、その過程において当該 AI システムを運用する過程として理解されるべきである。AI システムは、異なるレベルの自律性をもって運用するために設計されており、そのことは、AI システムが、ある程度まで、人間の関与から独立したふるまいをもち、また、人間の介入なしの運用の実現能力をもつことを意味する。設置の後に AI システムが発揮し得る適応性とは、当該システムが利用中に変化できるようにする自己学習の実現能力のことを指す。AI システムは、スタンドアロンベースで利用され得るのであり、または、当該システムが当該製品の中に物理的に統合されているか(組込)、当該製品の中に統合されることなく当該製品の機能性を提供するか(非組込)の別を問わず、製品のコンポーネントとして利用され得る。

¹⁵⁾ デジタルサービスのための単一市場に関する、及び、指令 2000/31/EC を改正する欧州議会及び理事会の 2022 年 10 月 19 日の規則(EU)2022/2065 (デジタルサービス法)(OJ L277, 27.10.2022, p. 1).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)(OJ L277, 27.10.2022, p. 1).

The notion of ‘AI system’ in this Regulation should be clearly defined and should be closely aligned with the work of international organisations working on AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in this field. Moreover, the definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling. The term ‘machine-based’ refers to the fact that AI systems run on machines. The reference to explicit or implicit objectives underscores that AI systems can operate according to explicit defined objectives or to implicit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific context. For the purposes of this Regulation, environments should be understood to be the contexts in which the AI systems operate, whereas outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions. AI systems are designed to operate with varying levels of autonomy, meaning that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention. The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use. AI systems can be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serves the functionality of the product without being integrated therein (non-embedded).

- (13) この規則の中で示される「設置者」の概念は、私的で非職業上の活動の過程において当該 AI システムが利用される場合を除き、行政機関、行政部局またはそれら以外の組織を含め、その者の権限に基づいて AI システムを利用する自然人または法人として解釈されるべきである。AI システムのタイプの相違により、そのシステムの利用は、設置者以外の者に対して影響を与え得る。

The notion of ‘deployer’ referred to in this Regulation should be interpreted as any natural or legal person, including a public authority, agency or other body, using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity. Depending on the type of AI system, the use of the system may affect persons other than the deployer:

- (14) この規則の中で用いられる「生体要素データ」の概念は、規則(EU) 2016/679の第4条第14号、規則(EU) 2018/1725の第3条第18号及び指令(EU) 2016/680の第3条第13号に定義する生体要素データの概念に照らして解釈されるべきである。生体要素データは、自然人の認証、識別または類型への振分けをできるようにし、また、自然人の感情の認識をできるようにし得る。

The notion of ‘biometric data’ used in this Regulation should be interpreted in light of the notion of biometric data as

defined in Article 4, point (14) of Regulation (EU) 2016/679, Article 3, point (18) of Regulation (EU) 2018/1725 and Article 3, point (13) of Directive (EU) 2016/680. Biometric data can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons.

- (15) この規則の中で示される「生体要素識別」の概念は、当該個人がその個人の同意を与えたか否かを問わず、当該個人の生体要素データと参照データベース内に記録保存されている個人の生体要素データとを照合することによって個人の同一性を確定するという目的のために、顔、眼の動き、体形、声、韻律、歩き方、姿勢、心拍数、血圧、匂い、打鍵の特徴のような、身体上、心理上及び行動上の人間の性状の自動化された認識として定義されるべきである。この概念は、生体要素の検証のために利用されることを意図する AI システムであって、認証を含んでおり、特定の自然人が、彼もしくは彼女がその者であると主張する者であることを確認すること、及び、あるサービスへのアクセスをもつこと、機器のロックを解除することまたは施設へのセキュリティアクセスをもつという目的のみのために自然人の同一性を確認することをそのシステムの単独の目的とするものを除外する。

The notion of ‘biometric identification’ referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human **features** such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual’s identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that **a specific natural person is the person he or she claims to be** and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.

- (16) この規則の中で示される「生体要素類型への振分け」の概念は、当該自然人の生体要素データを基礎として、自然人を特別の類型に割当てることとして定義されるべきである。そのような特別の類型は、性、年齢、髪の色、眼の色、刺青、行動上の特性もしくは性格上の特性、言語、信教、国内の少数派の一員であること、性的指向または政治的な指向のような側面と関連し得る。この概念は、客観的な技術上の理由により主たるサービスなしには当該機能が利用され得ないということ意味する別の商業システムと本質的に結びつけられた純粋に補助的な機能であり、かつ、当該機能または機能性を統合することがこの規則の規定の適用可能性を回避するための手段ではない生体要素類型への振分けシステムを含まない。例えば、オンライン市場で利用される顔または身体の特徴を分類するフィルタは、消費者が彼または彼女自身の前で当該製品の表示をプレビューできるようにすることによって、製品の販売過程を組成する主たるサービスとの関係においてのみそれが利用され得るのであり、かつ、その消費者が購入の判断をすることを助けるので、そのような補助的な機能を組成し得る。利用者が写真またはビデオを追加または修正できるようにするために顔または身体の特徴を振分けするオンラインソーシャルネットワーク上で利用されるフィルタもまた、オンラインのコンテンツ共有を組成す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しにはそのようなフィルタが利用され得ないので、補助的な機能として判断され得る。

The notion of ‘biometric categorisation’ referred to in this Regulation should be defined as assigning natural persons to

specific categories on the basis of their biometric data. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation. This does not include biometric categorisation systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, filters categorising facial or body features used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product **on him or herself** and help the consumer to make a purchase decision. Filters used on online social network services which categorise facial or body features to allow users to add or modify pictures or videos could also be considered to be ancillary feature as such filter cannot be used without the principal service of the social network services consisting in the sharing of content online.

- (17) この規則の中で示される「リモート生体要素識別システム」の概念は、典型的には隔地者間で、特別の技術、プロセスまたは使用される生体要素データのタイプの別を問わず、ある個人の生体要素データと参照データベース内に格納されている生体要素データとの照合によって、当該自然人の能動的な関与なしに、自然人の識別を意図する AI システムとして、機能的に定義されるべきである。そのようなリモート生体要素識別システムは、当該自然人の能動的な関与なしに、自然人の識別を大きく容易にするため、複数の人々またはそれらの人々の行動を同時に知覚するために典型的に利用される。この概念は、認証を含んでおり、生体要素の検証のために利用されることを意図する AI システムであって、特定の自然人が、彼もしくは彼女がその者であると主張する者であることを確認することのみをその AI システムの目的とするもの、及び、あるサービスへのアクセスをもつこと、機器のロックを解除することまたは施設へのセキュリティアクセスをもつことのために自然人の同一性を確認することをそのシステムの単独の目的とするものを除外する。その除外は、当該自然人の能動的な関与なしに、多数の個人の生体要素データの処理のために利用され得るリモート生体要素識別システムと比較して、そのようなシステムが、自然人の基本的な権利に対して軽微な影響しかもちそうにないということによって正当化される。リアルタイムのシステムの場合、生体要素データの取得、照合及び識別は、全て即時に、ほぼ即時に、または、いかなる場合においても大きな時間的経過なく発生する。この点に関し、軽微な時間的経過を定めることによって、関係する AI システムのリアルタイムの利用に関してこの規則の規定を回避する余地があってはならない。リアルタイムのシステムは、ビデオ映像記録のような、カメラによってまたはそれと類似の機能性をもつそれ以外の機器によって生成される「同時」または「ほぼ同時」の素材の利用を含む。それとは対照的に、「事後」のシステムの場合、生体要素データは既に取得されており、かつ、対照及び識別は、大きな時間経過の後に限り発生する。この素材は、閉回路テレビカメラまたは私用機器によって生成された画像またはビデオ映像記録のような、関係する自然人との関係における当該システムの利用よりも前に生成された素材を含む。

The notion of ‘remote biometric identification system’ referred to in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons without their active involvement, typically at a distance, through the comparison of a person’s biometric data with the biometric data contained in a reference database, irrespectively of the particular technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviour simultaneously in order to

facilitate significantly the identification of natural persons without their active involvement. This excludes AI systems intended to be used for biometric verification, **which includes authentication**, the sole purpose of which is to confirm that **a specific natural person is the person he or she claims to be** and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises. That exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to the remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons without their active involvement. In the case of **'real-time'** systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the **'real-time'** use of the AI systems concerned by providing for minor delays. **'Real-time'** systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data has already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

- (18) この規則の中で示される「感情認識システム」の概念は、当該自然人の生体要素データを基礎として自然人の感情または意図を識別するまたは推測するという目的のための AI システムとして定義されるべきである。この概念は、幸福、悲哀、怒り、驚愕、嫌悪、当惑、興奮、恥辱、軽蔑、満足及び歓楽のような感情または意図のことを指す。この概念は、例えば、事故防止の目的のために、職業操縦士または職業運転士の疲労状態の検出において利用されるシステム含め、痛みまたは疲労のような身体の状態を含まない。この概念は、感情を識別するまたは推論するために当該システムが利用される場合を除き、自明的にわかる表現、挙動または動作の単なる検出も含まない。それらの表現は、しかめ面もしくは笑顔のような基本的な顔の表現、または、手、腕もしくは頭部の動作のような挙動、または、声の高まりまたは静まりのような個人の声の特徴であり得る。

The notion of 'emotion recognition system' referred to in this Regulation should be defined as an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. It does not include physical states, such as pain or fatigue, including for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents. This does also not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.

- (19) この規則の目的のために、「公衆がアクセス可能な場所」の概念は、不特定数の自然人にとってアクセス可能な物理的な場所を指すものとして理解されるべきであり、かつ、その場所が私有であるか公有であるかを問わず、かつ、例えば、店舗、レストラン、喫茶店のような商業のため;例えば、銀行、職業上の活動、歓待のようなサービスのため;例えば、水泳プール、ジム、競技場のようなスポーツのた

め;例えば、バス、地下鉄及び鉄道駅、空港、輸送手段のような輸送のため;例えば、映画館、劇場、博物館、演奏会場及び会議場のような娯楽のため;または、例えば、公道及び広場、公園、森林、遊び場のようなレジャーまたはそれら以外のためのよう、その場所が利用され得る活動の別を問わない。潜在的な能力上または防護上の制限に拘わらず、切符購入もしくは輸送資格、事前登録または一定年齢であることのような予め定められ、不特定数の者によって満たされ得る一定の条件にアクセスが服するときも、場所は、公衆がアクセス可能であるとして分類されるべきである。対照的に、公共の安全もしくは保安と直接に関係する欧州連合法もしくは国内法により、または、当該の場所に対して関連する権限をもつ者による意思の明確な表明により、特定の定義された自然人にアクセスが制限されるときは、場所は、公衆がアクセス可能であると判断されてはならない。無施錠のドア、フェンス内に開かれた門のように、事実上アクセスできるということだけでは、アクセスを禁止または制限する標識のような反対のことを示す兆候や状況のある場所に公衆がアクセス可能であることを含意しない。関連する従業員及びサービス提供者のみによってアクセスされることが意図されている会社施設及び工場施設並びに事務室及び就労場所は、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、刑務所または出入国管理当局を含めてはならない。それら以外の、医院または空港にアクセスするために必要な私有住居建物の廊下のような幾つかの場所は、公衆がアクセス可能な場所及びアクセス可能ではない場所の両者を組成し得る。オンライン空間は、当該空間が物理的な空間ではないので、包摂されない。ただし、当の場に公衆がアクセス可能であるか否かは、問題となる個々の状況の特徴を考慮に入れ、ケースバイケースで判定されるべきである。

For the purposes of this Regulation the notion of ‘publicly accessible space’ should be understood as referring to any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned, irrespective of the activity for which the space may be used, such as for commerce, for example, shops, restaurants, cafés; for services, for example, banks, professional activities, hospitality; for sport, for example, swimming pools, gyms, stadiums; for transport, for example, bus, metro and railway stations, airports, means of transport; for entertainment, for example, cinemas, theatres, museums, concert and conference halls; or for leisure or otherwise, for example, public roads and squares, parks, forests, playgrounds. A space should also be classified as being publicly accessible if, regardless of potential capacity or security restrictions, access is subject to certain predetermined conditions which can be fulfilled by an undetermined number of persons, such as the purchase of a ticket or title of transport, prior registration or having a certain age. In contrast, a space should not be considered to be publicly accessible if access is limited to specific and defined natural persons through either Union or national law directly related to public safety or security or through the clear manifestation of will by the person having the relevant authority over the space. The factual possibility of access alone, such as an unlocked door or an open gate in a fence, does not imply that the space is publicly accessible in the presence of indications or circumstances suggesting the contrary, such as signs prohibiting or restricting access. Company and factory premises, as well as offices and workplaces that are intended to be accessed only by relevant employees and service providers, are spaces that are not publicly accessible. Publicly accessible spaces should not include prisons or border control. Some other spaces may comprise both publicly accessible and non-publicly accessible spaces, such as the hallway of a private residential building necessary to access a doctor’s office or an airport. Online spaces are not covered, as they are not physical spaces. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

- (20) 基本的な権利、健康及び安全を保護しつつ、AI システムから最大の受益を得るため、そして、民主的な管理を可能化するため、AI リテラシは、提供者、設置者及び影響を受ける個人に対し、AI システムと関連する説明を受けた上での判断を行うために必要となる概念を具備させるべきである。それらの概念は、関連する文脈との関係において異なるものであるかもしれないが、また、AI システムの開発段階の間における技術上の諸要素の正確な適用を理解すること、当該 AI システムの利用の間に適用される手段、当該 AI システムの出力を解釈するための適切な方法、及び、影響を受ける個人に関しては、AI の補助によって行われる判定が当該個人に対してどのような影響を与えることとなるかを理解するために必要となる知識を含み得る。この規則の適用の過程において、AI リテラシは、AI の価値連鎖の中にある全ての関与者に対し、適切な遵守とこの規則の正確な執行を確保するために求められる洞察を提供すべきである。更に、AI リテラシの措置の広範な実装及び適切な事後対応活動の導入は、労働条件の改善に貢献し、そして、究極的には、統合を支え、欧州連合における信頼できる AI の技術革新の途を支え得る。欧州人工知能委員会(「委員会」)は、AI リテラシツールを向上させ、AI システムの利用と関係する受益、リスク、安全確保、権利及び義務についての公衆の認識と理解を向上させるため、欧州委員会を支えるべきである。適格な利害関係者と協力して、欧州委員会及び構成国は、AI の開発、運用及び利用とかわる者の間における AI リテラシを高度化させるための任意の行動準則を作成することを促進すべきである。

In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems. Those notions may vary with regard to the relevant context and can include understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use, the suitable ways in which to interpret the AI system's output, and, in the case of affected persons, the knowledge necessary to understand how decisions taken with the assistance of AI will have an impact on them. In the context of the application this Regulation, AI literacy should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement. Furthermore, the wide implementation of AI literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately sustain the consolidation, and innovation path of trustworthy AI in the Union. The European Artificial Intelligence Board (the 'Board') should support the Commission, to promote AI literacy tools, public awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems. In cooperation with the relevant stakeholders, the Commission and the Member States should facilitate the drawing up of voluntary codes of conduct to advance AI literacy among persons dealing with the development, operation and use of AI.

- (21) 平等な競争の場を確保するため、そして、欧州連合全域にわたる個人の権利及び自由の実効的な保護を確保するため、この規則によって設けられる規定は、当該提供者が欧州連合内に拠点をもつか第三国内に拠点をもつかを問わず、AI システムの提供者に対して非差別の態様で適用されるべきであり、かつ、欧州連合内に拠点をもつ AI システムの設置者に対して適用されるべきである。

In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner;

irrespective of whether they are established within the Union or in a third country, and to deployers of AI systems established within the Union.

- (22) AI システムのデジタルな性質に照らし、一定の AI システムは、欧州連合内において当該システムが市場に置かれておらず、サービスに供されておらず、または、利用されていない場合であっても、この規則の適用範囲内にあるべきである。例えば、欧州連合内に拠点をもつ運用者が、高リスクとして分類されるような AI システムによって遂行される活動との関係において第三国内に拠点をもつ運用者に対して一定のサービス提供を契約する場合はそのような場合に該当する。当該状況において、当該運用者によって第三国内において利用される AI システムは、欧州連合内で適法に収集され、欧州連合から移転されたデータを処理でき、また、当該 AI システムが欧州連合内において市場に置かれ、サービスに供され、または、利用されることなしに、欧州連合内の締約運用者に対し、当該処理から生ずる当該 AI システムの出力を提供し得る。この規則の回避を防止するため、そして、欧州連合内に所在する自然人の実効性のある保護を確保するため、この規則は、当該 AI システムによって生産される出力が欧州連合内において利用されることが意図されている限り、第三国内に拠点をもつ AI システムの提供者及び設置者に対しても適用されるべきである。ただし、その者との間で情報及び証拠が交換される外国のパートナーとの間の将来の協力に関する既存の協定と特別の必要性を考慮に入れるため、当該第三国または国際組織が個人の基本的な権利及び自由の保護に関する十分な安全確保を提供することを条件として、欧州連合との間もしくは構成国との間の法執行及び法務上の協力のために欧州連合レベルもしくは国内レベルで締結された協力枠組み内または国際協定内で行動するときは、この規則は、第三国の行政機関及び国際組織に対して適用されるべきではない。それが適切なき場合は、このことは、そのような法執行及び法務上の協力を支える個別の職務を実施することを第三国から委任された法主体の活動に対しても適用され得る。そのような協力枠組みまたは協定は、構成国と第三国との間において、または、欧州連合、Europol 及びそれ以外の欧州連合の部局と第三国及び国際組織との間において、二国間で設けられてきた。この規則の下において法執行機関及び法務当局の監督に関する職務権限のある機関は、当該協力枠組み及び国際協定が個人の基本的な権利及び自由の保護と関する十分な安全確保を含んでいるか否かを評価すべきである。欧州連合内においてそのような出力を活用する受け手である国内機関並びに欧州連合の機関、組織、事務局及び部局は、それらの利用が欧州連合法を遵守することを確保することについて責任を負い続ける。将来においてそれらの国際協定が改正されまたは新たな国際協定が締結されるときは、その締約者は、それらの協定をこの規則の要件に揃えるための最大限の努力を尽くすべきである。

In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are not placed on the market, put into service, or used in the Union. This is the case, for example, where an operator established in the Union contracts certain services to an operator established in a third country in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used in a third country by the operator could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers

of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union. Nonetheless, to take into account existing arrangements and special needs for future cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of cooperation or international agreements concluded at Union or national level for law enforcement and judicial cooperation with the Union or the Member States, provided that the relevant third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Where relevant, this may cover activities of entities entrusted by the third countries to carry out specific tasks in support of such law enforcement and judicial cooperation. Such framework for cooperation or agreements have been established bilaterally between Member States and third countries or between the European Union, Europol and other Union agencies and third countries and international organisations. The authorities competent for supervision of the law enforcement and judicial authorities under this Regulation should assess whether those frameworks for cooperation or international agreements include adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Recipient national authorities and Union institutions, bodies, offices and agencies making use of such outputs in the Union remain accountable to ensure their use complies with Union law. When those international agreements are revised or new ones are concluded in the future, the contracting parties should make utmost efforts to align those agreements with the requirements of this Regulation.

- (23) AI システムの提供者または設置者として行動する場合、この規則は、欧州連合の機関、組織、事務局及び部局に対しても適用されるべきである。

This Regulation should also apply to Union institutions, bodies, offices and agencies when acting as a provider or deployer of an AI system.

- (24) 軍、国防または国家安全保障の目的のためにそのようなシステムを修正した上でまたは修正せずに AI システムが市場に置かれ、サービスに供されまたは利用される場合においては、その限りにおいて、その法主体が公的な法主体であるか民間の法主体であるかといったような、どのタイプの法主体が当該活動を実施しているかに拘わらず、その AI システムは、この規則の適用範囲から除外されるべきである。軍及び国防の目的に関し、そのような適用除外は、TEU の第 4 条第 2 項によって並びに TEU の第 V 款第 2 章に含まれている構成国の国防基本方針及び欧州連合の共通国防基本方針の特性によって、それら両者によって正当化されるのであり、それらは、国際公法に服している。それゆえ、それらは、破壊力の行使という文脈における AI システムの規律のための及び破壊力の行使以外の軍及び国防の活動という文脈における AI システムの規律のための、より適切な法的枠組みである。国家安全保障の目的に関し、この適用除外は、TEU の第 4 条第 2 項に従って国家安全保障が構成国の単独の責務のままとされていることによって並びに国家安全保障上の活動の特性及び業務運営上の必要性とそれらの活動に対して適用可能な個別の国内規定の両者によって、それら両者によって正当化される。ただし、軍、国防または国家安全保障の目的のために開発され、市場に置かれ、サービスに供されまたは利用される AI システムが、例えば、民間の目的または人道上の目的、法執行の目的または公共の保安の目的のような別の目的のために一時的にまたは恒久的に利用される場合、そのようなシステムは、この規則の適用範囲内にあるだろう。その場合におい

ては、軍、国防または国家安全保障の目的以外の目的のためにその AI システムを利用する法主体は、そのシステムが既にこの規則を遵守している場合を除き、その AI システムがこの規則を遵守することを確保すべきである。適用除外される諸目的、すなわち、軍、国防または国家安全保障の目的のために、かつ、例えば、民間の目的または法執行のような 1 または複数の適用除外されない目的のために市場に置かれまたはサービスに供される AI システムは、この規則の適用範囲内にあり、当該システムの提供者は、この規則の遵守を確保すべきである。それらの場合において、ある AI システムがこの規則の適用範囲内にあるかもしれないということは、国家安全保障、国防及び軍の活動を遂行する法主体のタイプの違いに拘わらず、それらの活動を遂行する法主体が、その利用がこの規則の適用範囲から除外されている AI システムを国家安全保障、軍及び国防の目的のために利用できることに対して影響を与えてはならない。民間の目的または法執行の目的のために市場に置かれ、軍、国防または国家安全保障の目的のために修正した上でまたは修正せずに利用される AI システムは、それらの活動を遂行する法主体のタイプの違いに拘わらず、この規則の適用範囲内にあるとしてはならない。

If, and insofar as, AI systems are placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes, those should be excluded from the scope of this Regulation regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity. As regards military and defence purposes, such exclusion is justified both by Article 4(2) TEU and by the specificities of the Member States' and the common Union defence policy covered by Chapter 2 of Title V TEU that are subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes is used outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the AI system for other than military, defence or national security purposes should ensure the compliance of the AI system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, and one or more non-excluded purposes, such as civilian purposes or law enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance with this Regulation. In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out national security, defence and military activities, regardless of the type of entity carrying out those activities, to use AI systems for national security, military and defence purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the market for civilian or law enforcement purposes which is used with or without modification for military, defence or national security purposes should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities.

- (25) この規則は、技術革新を支えるべきであり、科学の自由を尊重すべきであり、そして、調査研究及び開発の活動を損ねてはならない。それゆえ、科学の調査研究及び開発という目的のみのために個

別に開発され及びサービスに供される AI システム及びモデルをこの規則の適用範囲から除外する必要がある。それに加えて、市場に置かれまたはサービスに供される前に、AI システムまたはモデルに関する科学の調査研究及び開発の活動に対してこの規則が格別影響を与えることがないことを確保する必要がある。製品化に向けた AI システム及びモデルと関連する調査研究、試験及び開発の活動に関してもまた、当該システム及びモデルがサービスに供されまたは市場に置かれる前に、この規則の条項が適用されてはならない。その適用除外は、そのような調査研究及び開発の活動の結果として、この規則の適用範囲内にある AI システムが市場に置かれまたはサービスに供される場合においてこの規則を遵守すべき義務を妨げず、また、AI 法制サンドボックス及び実世界条件下の試験に関する条項の適用を妨げない。更に、科学の調査研究及び開発という目的のみのために個別に開発され及びサービスに供される AI システムの適用除外を妨げることなく、それ以外の、調査研究及び開発の活動の実施のために利用され得る AI システムは、この規則の条項に服するままであるべきである。いかなる場合においても、いかなる調査研究及び開発の活動も、科学の調査研究に関する承認された倫理基準及び職業上の基準に従って遂行されるべきであり、かつ、適用可能な欧州連合法に従って実施されるべきである。

This Regulation should support innovation, should respect freedom of science, and should not undermine research and development activity. It is therefore necessary to exclude from its scope AI systems and models specifically developed and put into service for the sole purpose of scientific research and development. Moreover, it is necessary to ensure that this Regulation does not otherwise affect scientific research and development activity on AI systems or models prior to being placed on the market or put into service. As regards product-oriented research, testing and development activity regarding AI systems or models, the provisions of this Regulation should also not apply prior to those systems and models being put into service or placed on the market. That exclusion is without prejudice to the obligation to comply with this Regulation where an AI system falling into the scope of this Regulation is placed on the market or put into service as a result of such research and development activity and to the application of provisions on AI regulatory sandboxes and testing in real world conditions. Furthermore, without prejudice to the exclusion of AI systems specifically developed and put into service for the sole purpose of scientific research and development, any other AI system that may be used for the conduct of any research and development activity should remain subject to the provisions of this Regulation. In any event, any research and development activity should be carried out in accordance with recognised ethical and professional standards for scientific research and should be conducted in accordance with applicable Union law.

- (26) AI システムに関する拘束力のある規定の比例的かつ実効的なセットを導入するため、明確に定義されたリスクベースのアプローチに従うべきである。そのアプローチは、そのような規定のタイプ及び内容を、AI システムが生成し得るリスクの脅威度及び範囲に合わせるべきである。それゆえ、一定の許容できない AI 実務を禁止すること、高リスク AI システムの要件及び関連運用者の義務を定めること、そして、一定の AI システムに関する透明性義務を定めることが必要である。

In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain unacceptable AI practices, to lay down

requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.

- (27) リスクベースのアプローチは拘束力のある規定の比例的かつ実効的なセットの基礎であるが、欧州委員会によって任命された独立の AI HLEG によって策定された信頼できる AI に関する 2019 年の倫理指針を想起することが大事である。同倫理指針の中において、AIHLEG は、AI に関する 7 つの拘束力のない倫理上の基本原則を策定した。それらは、AI が信頼できかつ倫理的に良好であることを確保することを助けることが意図されている。7 つの基本原則は、人間の代理者であることと人間による監視;技術上の堅牢性と安全性;プライバシーとデータ統治;透明性;多様性、非差別と公正性;社会と環境の良好な状態及び説明責任を含めている。この規則及びそれ以外の適用可能な欧州連合法の法的拘束力のある要件を妨げることなく、同倫理指針は、憲章に沿って、かつ、欧州連合が基礎とする価値に沿って、一貫性があり、信頼できかつ人間中心の AI の設計に寄与する。AI HLEG の指針によれば、人間の代理者であることと人間による監視とは、人々に対して奉仕し、人間の尊厳と個人の自律性を尊重し、かつ、人間によって適切に管理及び監視され得る方法で稼働するツールとして AI システムが開発され及び利用されることを意味する。技術上の堅牢性と安全性とは、問題発生の場合の堅牢性があるようにし、かつ、第三者によって違法な利用ができるようにするための当該 AI システムの利用または性能を改変する試みに抗する回復力があるようにし、かつ、意図していない危険を最小化するような方法で AI システムが開発され及び利用されることを意味する。プライバシー及びデータ統治とは、データの処理が品質及び完全性の面における高度な基準に適合しつつ、プライバシー及びデータ保護の諸規定に従って AI システムが開発され及び利用されることを意味する。透明性とは、人間が AI システムとの間で通信またはやりとりしていることを人間に気付かせるようにしつつ、並びに、当該 AI システムの実現能力及び限界を設置者に対して適正に情報提供しつつ、また、影響を受ける個人に対して当該個人の権利を適正に知らせつつ、適切な追跡可能性と説明可能性があるような方法で AI システムが開発され及び利用されることを意味する。多様性、非差別及び公正性とは、欧州連合法または国内法によって禁止されている差別的な影響及び不公正なバイアスを避けつつ、多様な関与者を包摂し、かつ、平等なアクセス、ジェンダーの平等及び文化の多様性を向上させるような方法で AI システムが開発され及び利用されることを意味する。社会と環境の良好な状態とは、個人、社会及び民主主義に対する長期的な影響を監視及び評価しつつ、持続可能であり、環境フレンドリーな態様であり、かつ、全ての人間に受益させるような方法で AI システムが開発され及び利用されることを意味する。それらの基本原則の適用は、それが可能なときは、AI モデルの設計及び利用において翻訳されるべきである。同基本原則は、いかなる場合においても、この規則の下にある行動準則の起草のための基礎として奉仕すべきである。産業界、学術、市民社会団体及び標準化の組織を含め、全ての利害関係者は、任意のベストプラクティス及び技術標準の策定のために、この倫理上の基本原則をしかるべく考慮に入れることが推奨される。

While the risk-based approach is the basis for a proportionate and effective set of binding rules, it is important to recall the 2019 Ethics guidelines for trustworthy AI developed by the independent AI HLEG appointed by the Commission. In those guidelines, the AI HLEG developed seven non-binding ethical principles for AI which are intended to help ensure that AI is trustworthy and ethically sound. The seven principles include human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal

and environmental well-being and accountability. Without prejudice to the legally binding requirements of this Regulation and any other applicable Union law, those guidelines contribute to the design of coherent, trustworthy and human-centric AI, in line with the Charter and with the values on which the Union is founded. According to the guidelines of the AIHLEG, human agency and oversight means that AI systems are developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans. Technical robustness and safety means that AI systems are developed and used in a way that allows robustness in the case of problems and resilience against attempts to alter the use or performance of the AI system so as to allow unlawful use by third parties, and minimise unintended harm. Privacy and data governance means that AI systems are developed and used in accordance with privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity. Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights. Diversity, non-discrimination and fairness means that AI systems are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law. Social and environmental well-being means that AI systems are developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy. The application of those principles should be translated, when possible, in the design and use of AI models. They should in any case serve as a basis for the drafting of codes of conduct under this Regulation. All stakeholders, including industry, academia, civil society and standardisation organisations, are encouraged to take into account, as appropriate, the ethical principles for the development of voluntary best practices and standards.

- (28) AI の多数の有益な利用をひとまず措き, AI は, 濫用され得るものでもあり, また, 操作, 搾取及び社会監視の実務のための革新的かつ強力なツールも提供し得る。そのような実務は, とりわけ危険かつ侵害的であり, かつ, それらの実務は, 非差別, データ保護及びプライバシーの権利並びに児童の権利を含め, 人間の尊厳の尊重, 自由, 平等, 民主主義及び法の支配並びに憲章に掲げられた基本的な権利という欧州連合の価値と矛盾するものなので, 禁止されるべきである。

Aside from the many beneficial uses of AI, it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and abusive and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, including the right to non-discrimination, to data protection and to privacy and the rights of the child.

- (29) AI によって実現可能にされた操作の技法は, 望まない行動に従事するように人々を仕向けるため, または, 人々の自律性, 意思決定及び自由な選択を毀損し及び損ねる方法で人々に対して判断を促すことにより人々を騙すために利用され得る。それゆえ, 人の行動を実質的に歪める目的またはその効果をもち, それらの目的または効果によって, とりわけ, 身体, 精神上の健康または財産上の利益に対する十分な大きさの負の影響をもつ大きな危険を発生させるおそれのある一定の AI シス

テムを市場に置くこと、サービスに供すること、または、利用することは、とりわけ危険であり、禁止されるべきである。そのような AI システムは、それらの刺激が人間の知覚を超えているために個人が気付くことのできない音響、画像、ビデオの刺激のようなサブリミナルのコンポーネントを具備しており、または、それ以外の、当該技法に人々が意識的に気付かない方法で、または、人々がそれらの技法に気付いているときでさえ、なお欺瞞的でありもしくは管理や抵抗ができない方法で、個人の自律性、意思決定または自由な選択を毀損または損ねる操作的または欺瞞的な技法を具備している。例えば、当該インタフェイスまたは仮想現実が大きく危険な態様で当該個人の行動を実質的に歪めることがあり得る範囲内において、機械と生体脳間のインタフェイスまたは仮想現実、どの刺激が個人に対して提示されるのかを高いレベルで管理できるので、機械と生体脳間のインタフェイスまたは仮想現実によってこのことが促進され得る。加えて、それ以外に、AI システムは、当該個人の年齢、欧州議会及び理事会の指令(EU) 2019/882¹⁶の意味における障害、または、極端に貧困な状態で生活している個人、人種上もしくは信教上の少数者のような、悪用に対して当該個人をより脆弱にしてしまうような個別の社会状況もしくは経済状況のゆえに、個人または特定の個人のグループの脆弱性も悪用し得る。それゆえ、そのような AI システムは、個人の行動を実質的に歪める目的またはその効果をもち、かつ、当該個人もしくは他の個人または個人のグループに対し、経年的に累積される可能性のある危険を含め、大きな危険を生じさせまたは大きな危険を生じさせる合理的な可能性のある態様で、市場に置かれ、サービスに供され、または、利用され得るのであり、禁止されるべきである。当該 AI システムの外にある要因であって、その提供者または設置者の管理の外にある要因、すなわち、合理的に予想され得ず、それゆえ、当該 AI システムの提供者または設置者によっては緩和され得ない要因から当該歪みが生じている場合、行動を歪める意図が存在していることは推定され得ない。いかなる場合においても、AI によって実現可能にされた操作的または悪用的な実務からそのような危険が生じていることを条件として、その提供者または設置者に関し、大きな危険を生じさせる意図をもつことを必要としない。そのような AI 実務の禁止は、欧州議会及び理事会の指令 2005/29/EC¹⁷に含まれている条項を補完し、とりわけ、AI システムを通じて当該実務が置かれているかそれ以外の場合であるかを問わず全ての状況下において、消費者に対して経済上または金銭上の危険をもたらす商業上の不公正な実務が禁止されていることを補完する。この規則における操作的な実務及び悪用的な実務の禁止は、当該医療実務が適用可能な法律及び医療水準に従って、例えば、個人またはその個人の適法な代理者の明示の同意に従って実施されているときは、精神療法の心理療法または身体リハビリテーションのような医療行為の過程における適法な実務に対して影響

¹⁶ 製品及びサービスのアクセシビリティ要件に関する欧州議会及び理事会の 2019 年 4 月 17 日の指令(EU) 2019/882(OJ L151, 7.6.2019, p. 70).

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

¹⁷ 域内市場における企業と消費者間の不公正な商業実務に関する、理事会指令 84/450/EEC、欧州議会及び理事会の指令 97/7/EC、指令 98/27/EC 及び指令 2002/65/EC 並びに欧州議会及び理事会の規則(EC) No 2006/2004を改正する欧州議会及び理事会の 2005 年 5 月 11 日の指令 2005/29/EC (「不公正な商業実務指令」)(OJ L 149, 11.6.2005, p. 22).

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')(OJ L 149, 11.6.2005, p. 22).

を与えてはならない。加えて、例えば、宣伝広告の分野において、普通の合法的な商業上の実務であって、適用可能な法律を遵守するものは、それ自体としては、AI によって実現可能にされた危険で操作的な実務を組成していると判断されてはならない。

AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that **subverts and impairs** their autonomy, decision-making and free choices. The placing on the market, the putting into service or the use of certain AI systems with the objective to or the effect of materially distorting human behaviour, whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur, are particularly dangerous and should therefore be prohibited. Such AI systems deploy subliminal components such as audio, image, video stimuli that persons cannot perceive, as those stimuli are beyond human perception, or other manipulative or deceptive techniques that **subvert or impair** person's autonomy, decision-making or free choice in ways that people are not consciously aware of those techniques or, where they are aware of them, can still be deceived or are not able to control or resist them. This could be facilitated, for example, by machine-brain interfaces or virtual reality as they allow for a higher degree of control of what stimuli are presented to persons, insofar as they may materially distort their behaviour in a significantly harmful manner. In addition, AI systems may also otherwise exploit the vulnerabilities of a person or a specific group of persons due to their age, disability within the meaning of Directive (EU) 2019/882 of the European Parliament and of the Council⁽¹⁶⁾, or a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minorities. Such AI systems can be placed on the market, put into service or used with the objective to or the effect of materially distorting the behaviour of a person and in a manner that causes or is reasonably likely to cause significant harm to that or another person or groups of persons, including harms that may be accumulated over time and should therefore be prohibited. It may not be possible to assume that there is an intention to distort behaviour where the distortion results from factors external to the AI system which are outside the control of the provider or the deployer, namely factors that may not be reasonably foreseeable and therefore not possible for the provider or the deployer of the AI system to mitigate. In any case, it is not necessary for the provider or the deployer to have the intention to cause significant harm, provided that such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices are complementary to the provisions contained in Directive 2005/29/EC of the European Parliament and of the Council⁽¹⁷⁾, in particular unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise. The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable law and medical standards, for example explicit consent of the individuals or their legal representatives. In addition, common and legitimate commercial practices, for example in the field of advertising, that comply with the applicable law should not, in themselves, be regarded as constituting harmful manipulative AI-enabled practices.

- (30) 個人の政治的意見、労働組合の加入、信教または信条、人種、性生活または性的指向を推測または推論するための、個々の個人の顔または指紋のような自然人の生体要素データを基礎とする生体要素類型への振分けシステムは、禁止されるべきである。この禁止は、髪の色または眼の色による

画像の整列のような、欧州連合法または国内法に沿って入手された生体要素のデータセットの生体要素データによる適法なラベリング、選別または振分けであって、例えば、法執行の分野において利用され得るものを包摂してはならない。

Biometric categorisation systems that are based on natural persons' biometric data, such as an individual person's face or fingerprint, to deduce or infer an individuals' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation should be prohibited. That prohibition should not cover the lawful labelling, filtering or categorisation of biometric data sets acquired in line with Union or national law according to biometric data, such as the sorting of images according to hair colour or eye colour, which can for example be used in the area of law enforcement.

- (31) 公的部門の関係者または民間の関与者による自然人の社会的得点評価を提供する AI システムは、差別的な成果と一定のグループの疎外を導き得る。それらの AI システムは、尊厳と非差別の権利及び平等と正義という価値に反し得る。そのような AI システムは、多角的な文脈における当該自然人または自然人のグループの社会的行動と関連する多角的なデータ得点または一定期間にわたる既知の、推論されたもしくは予測された個人もしくは性格の特徴と関連する多角的なデータ得点を基礎として、自然人または自然人のグループを評価または分類する。そのような AI システムに由来する社会得点評価は、そのデータが当初に生成または収集された文脈とは関係のない社会的文脈における自然人または自然人のグループ全体の有害または好ましくない取扱いを導き得るのであり、または、当該自然人または自然人のグループの社会的行動の重さに対して比例的ではない有害な取扱いもしくは正当化されない有害な取扱いを導き得る。それゆえ、そのような承認されない得点評価実務を伴い、かつ、そのような有害または好ましくない成果を導く AI システムは、禁止されるべきである。この禁止は、国内法及び欧州連合法に従う個別の目的のために遂行される自然人の適法な評価実務に対して影響を与えてはならない。

AI systems providing social scoring of natural persons by public or private actors may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify natural persons or groups thereof on the basis of multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. AI systems entailing such unacceptable scoring practices and leading to such detrimental or unfavourable outcomes should therefore be prohibited. That prohibition should not affect lawful evaluation practices of natural persons that are carried out for a specific purpose in accordance with Union and national law.

- (32) 法執行の目的のための公衆がアクセス可能な場所における自然人のリアルタイムのリモート生体要素識別のための AI システムの利用は、大部分の人々の私生活に対してそのシステムが影響を与え得る範囲内において、関係する個人の権利及び自由に対してとりわけ侵害的であり、常時監視の気

分を生じさせ、そして、集会の自由及びそれ以外の基本的な権利の行使を間接的に抑制する。自然人のリモート生体要素識別を意図する AI システムの技術上の不正確性は、バイアスのかかった結果を導き得るのであり、また、差別的な効果を伴い得る。そのようにしてあり得るバイアスのかかった結果及び差別的な効果は、とりわけ、年齢、民族、人種、性または障害と関連して特に適合性をもつ。加えて、その影響の即時性、及び、リアルタイムで運用されるそのようなシステムの利用に関して更に点検または訂正するための機会の限定性は、法執行活動の過程において関係する者または法執行活動によって影響を受ける者の権利及び自由に関し、より高められたリスクをもたらす。

The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities.

- (33) それゆえ、その重要性がそのリスクを上回る重要な公共の利益を達成するためにその利用が厳格に必要な限定的に列挙されかつ狭く定義された状況下にある場合を除き、法執行の目的のためのそれらの AI システムの利用は、禁止されるべきである。それらの状況は、失踪中の個人を含め、一定の犯罪被害者の捜索；自然人の生命もしくは身体の安全に対する一定の脅威またはテロ攻撃の一定の脅威；及び、当該犯罪行為が少なくとも 4 年を上限とする拘禁刑または拘束命令により関係する構成国において処罰可能であり、かつ、そのことが当該構成国の法律の中で定められているときは、この規則の別紙中に列挙する犯罪行為の加害者または被疑者の所在地特定または同一性識別を含む。国内法に従ったそのような拘禁刑または拘束命令の閾値は、リアルタイムのリモート生体要素識別システムの利用を潜在的に正当化するために当該侵害行為が十分に重大であるべきことを確保することに貢献する。それに加えて、実務上、それらの犯罪行為中の幾つかが関連性をもつ可能性がそれ以外の犯罪行為よりも高いこと、その場合、リアルタイムのリモート生体要素識別によることが必要になると予想され、かつ、列挙された異なる犯罪行為の加害者または被疑者の所在地特定または同一性識別の高度に異なる実務上の要求の程度と比例していることを考慮に入れた上で、かつ、危険または潜在的な負の結果の重大性、蓋然性及び規模のあり得る相違を考慮した上で、この規則の別紙中に定める犯罪行為のリストは、理事会枠組み決定 2002/584/JHA¹⁸の中で列挙されている 32 の犯罪行為を基礎としている。人々に対する基礎供給の提供を妨げる重大な危険または国家のコア機能の執行を妨げる重大な危険による場合を含め、そのような不可欠インフラの混

¹⁸ 欧州逮捕令状及び構成国間の身柄引渡し手続に関する 2002 年 6 月 13 日の理事会枠組み決定 2002/584/JHA (OJ L 190, 18.7.2002, p. 1).

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

乱または破壊が個人の生命または身体の安全に対する差し迫った脅威を帰結し得るときは、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、欧州議会及び理事会の指令(EU) 2022/2557¹⁹の第 2 条第 4 号に定義する不可欠インフラの重大な混乱からも生じ得る。加えて、この規則は、関係する個人の面前において、そのような検査に関する欧州連合法及び国内法に定める条件に従って、法執行機関、出入国管理当局、移民または難民当局が同一性識別検査を実施するための能力を維持すべきである。とりわけ、法執行機関、出入国管理当局、移民または難民当局は、同一性検査の間、事前の許可を得ることをこの規則によって要求されることなく、同一性を識別されることを拒否する者または当該の者の識別名を述べることができない者もしくは証明できない者の同一性を識別するために、欧州連合法または国内法に従って、情報システムを利用できるべきである。その者は、例えば、犯罪に関与した者であって、事故または病状のゆえに、当該の者の識別名を法執行機関に対して開示することが期待できない者または不可能な者であり得る。

The use of those systems for the purpose of law enforcement should therefore be prohibited, except in exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for certain victims of crime including missing persons; certain threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of perpetrators or suspects of the criminal offences listed in an annex to this Regulation, where those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years and as they are defined in the law of that Member State. Such a threshold for the custodial sentence or detention order in accordance with national law contributes to ensuring that the offence should be serious enough to potentially justify the use of ‘real-time’ remote biometric identification systems. Moreover, the list of criminal offences provided in an annex to this Regulation is based on the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA⁽¹⁸⁾, taking into account that some of those offences are, in practice, likely to be more relevant than others, in that the recourse to ‘real-time’ remote biometric identification could, foreseeably, be necessary and proportionate to highly varying degrees for the practical pursuit of the localisation or identification of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences. An imminent threat to life or the physical safety of natural persons could also result from a serious disruption of critical infrastructure, as defined in Article 2, point (4) of Directive (EU) 2022/2557 of the European Parliament and of the Council⁽¹⁹⁾, where the disruption or destruction of such critical infrastructure would result in an imminent threat to life or the physical safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core function of the State. In addition, this Regulation should preserve the ability for law enforcement, border control, immigration or asylum authorities to carry out identity checks in the presence of the person concerned in accordance with the conditions set out in Union and national law for such checks. In particular, law enforcement, border control, immigration or asylum authorities should be able to use information systems, in accordance with Union or national law, to identify persons who,

¹⁹ 不可欠法主体の回復力に関する、及び、理事会指令 2008/114/EC を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU)2022/2557 (OJL333, 27.12.2022, p. 164).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJL333, 27.12.2022, p. 164).

during an identity check, either refuse to be identified or are unable to state or prove their identity, without being required by this Regulation to obtain prior authorisation. This could be, for example, a person involved in a crime, being unwilling, or unable due to an accident or a medical condition, to disclose their identity to law enforcement authorities.

- (34) それらのシステムが責任のある比例的な態様で利用されることを確保するため、それら限定列挙されかつ狭く定義された個々の状況において、とりわけ、その要請を生じさせている状況の性質、及び、関係する全ての者の権利及び自由に対するその利用の結果、並びに、その利用に付随して定められる安全確保及び条件に関し、一定の要素が考慮に入れられるべきことを定めることも重要である。加えて、法執行の目的のための公衆がアクセス可能な場所におけるリアルタイムのリモート生体要素識別システムの利用は、とりわけ、脅威、被害者または加害者と関連する証拠または徴候を考慮し、個別に的を絞った個人の同一性を確認するためにのみ設置されるべきであり、かつ、期間並びに地理的範囲及び人的範囲に関して厳格に必要なところに限定されるべきである。公衆がアクセス可能な場所におけるリアルタイムのリモート生体要素識別システムの利用は、関連する法執行機関が、基本的な権利の影響評価を完了しており、かつ、この規則において別異に定めていない限り、この規則に定めるデータベースにそのシステムを登録した場合においてのみ、認められるべきである。個人の参照データベースは、上述の個々の状況における個々の利用にとって適切であるべきである。

In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be deployed only to confirm the specifically targeted individual's identity and should be limited to what is strictly necessary concerning the period of time, as well as the geographic and personal scope, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a fundamental rights impact assessment and, unless provided otherwise in this Regulation, has registered the system in the database as set out in this Regulation. The reference database of persons should be appropriate for each use case in each of the situations mentioned above.

- (35) 法執行の目的のための公衆がアクセス可能な場所におけるリアルタイムのリモート生体要素識別システムの個々の利用は、構成国の法務当局または独立の行政機関による、その判断が拘束力をもつ明示かつ個別の許可に服するべきである。そのような許可は、原則として、1 または複数の個人を識別するためのその AI システムの利用よりも前に得られるべきである。緊急性を根拠として適正に正当化される状況においては、すなわち、関係するシステムを利用する必要性が、その AI システムの利用を開始する前に許可を得ることを実効的かつ客観的に不可能とさせているような状況下においては、この原則に対する適用除外が許容されるべきである。そのような緊急の状況下において、AI システムの利用は、絶対的にミニマムに必要な範囲内に限定されるべきであり、また、国内法の中で定められており、かつ、個々の個別の緊急利用例の過程において当該法執行機関自身によって指定される適切な安全確保及び条件に服するべきである。加えて、法執行機関は、そのような状況下

においては、不適切な遅滞なくかつ遅くとも 24 時間以内に、より早い時点で許可を求められなかった理由を提供して、そのような許可を求めるべきである。そのような許可が取消されるときは、当該許可と結びつけられたリアルタイム生体要素識別システムの利用は、即時の効果をもって停止されるべきであり、かつ、そのような利用と関連する全てのデータは、破棄され及び削除されるべきである。そのようなデータは、そのようなシステムの利用の過程において AI システムによって直接に得られた入力データ、並びに、当該許可と結びつけられた利用の結果及び出力を含む。そのデータは、別の欧州連合法または国内法に従って適法に得られた入力を含めてはならない。いかなる場合においても、リモート生体要素識別システムの出力のみを基礎として、個人に対して負の法的影響を生成する判断が行われてはならない。

Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State whose decision is binding. Such authorisation should, in principle, be obtained prior to the use of the AI system with a view to identifying a person or persons. Exceptions to that rule should be allowed in duly justified situations on grounds of urgency, namely in situations where the need to use the systems concerned is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use of the AI system. In such situations of urgency, the use of the AI system should be restricted to the absolute minimum necessary and should be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations request such authorisation while providing the reasons for not having been able to request it earlier, without undue delay and at the latest within 24 hours. If such an authorisation is rejected, the use of real-time biometric identification systems linked to that authorisation should cease with immediate effect and all the data related to such use should be discarded and deleted. Such data includes input data directly acquired by an AI system in the course of the use of such system as well as the results and outputs of the use linked to that authorisation. It should not include input that is legally acquired in accordance with another Union or national law. In any case, no decision producing an adverse legal effect on a person should be taken based solely on the output of the remote biometric identification system.

- (36) この規則及び国内規定に定める要件に従って当該当局の職務を実行するため、適格な市場監視当局及び国内データ保護当局は、リアルタイム生体要素識別システムの個々の利用の通知を受けなければならない。通知を受けた市場監視当局及び国内データ保護当局は、欧州委員会に対し、リアルタイム生体要素識別システムの利用に関する年次報告書を提出すべきである。

In order to carry out their tasks in accordance with the requirements set out in this Regulation as well as in national rules, the relevant market surveillance authority and the national data protection authority should be notified of each use of the real-time biometric identification system. Market surveillance authorities and the national data protection authorities that have been notified should submit to the Commission an annual report on the use of real-time biometric identification systems.

- (37) 更に、関係する構成国が、当該構成国の国内法の細目規定の中でそのような利用を許可できること

を明示で定めることを決定した場合において、かつ、その決定の範囲内に限り、この規則によって定められる限定的な枠組みの範囲内におけるこの規則に従った構成国の領土内におけるそのような利用のみが可能であるべきことを定めることが適切である。その結果として、構成国は、この規則の下において、そのような可能性を全く定めないか、または、この規則の中で特定された許可を受けた利用を正当化可能な対象の幾つかに関してのみそのような可能性を定めるかの自由を維持する。そのような国内規定は、その採択から遅くとも 30 日以内に、欧州委員会に対して通知されるべきである。

Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State concerned has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation. Such national rules should be notified to the Commission within 30 days of their adoption.

- (38) 法執行の目的のための公衆がアクセス可能な場所における自然人のリアルタイムのリモート生体要素識別のための AI システムの利用は、必然的に、生体要素データの処理を含む。一定の適用除外に服して、TFEU の第 16 条を基礎としてそのような利用を禁止するこの規則の規定は、指令(EU) 2016/680 の第 10 条に含まれる生体要素データの処理に関する規定との関係において、そして、含まれている生体要素データのそのような利用及び処理を限定的な態様で規律する特別法として適用されるべきである。それゆえ、法執行の目的のために職務権限のある機関が行動する場合、その枠組みの外には、指令(EU) 2016/680 の第 10 条に列挙する根拠に基づいてそのようなシステムを利用するため及びそのようなシステムと関係するそのようなデータを処理するための当該職務権限のある機関のための適用範囲を存在させることなく、そのような利用及び処理は、この規則によって定められる枠組みと互換性がある範囲内に限り、可能であるべきである。この文脈において、この規則は、指令(EU) 2016/680 の第 8 条に基づく個人データの処理のための法律上の根拠を提供することを意図していない。ただし、職務権限のある機関による場合を含め、法執行以外の目的のための公衆がアクセス可能な場所におけるリアルタイムのリモート生体要素識別システムの利用は、この規則によって定められる法執行の目的のためのそのような利用と関連する個別の枠組みに包摂されてはならない。それゆえ、法執行以外の目的のためのそのような利用は、この規則に基づく許可の要件及びその許可に有効性を与えることができる国内法上の適用可能な細目規定に服させてはならない。

The use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should be possible only in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In that context, this Regulation is not intended to provide the legal basis for the processing of personal data

under Article 8 of Directive (EU) 2016/680. However, the use of real-time remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to that authorisation.

- (39) この規則によって規律される法執行の目的のための公衆がアクセス可能な場所におけるリアルタイムのリモート生体要素識別システムの利用と関係する場合以外においては、生体要素識別のための AI システムの利用に含まれる生体要素データ及びそれ以外の個人データの処理は、指令(EU) 2016/680 の第 10 条から帰結する全ての要件を遵守し続けるべきである。法執行以外の目的に関し、規則(EU) 2016/679 の第 9 条第 1 項及び規則(EU) 2018/1725 の第 10 条第 1 項は、それらの条項に定める限定的な適用除外に服して、生体要素データの処理を禁止している。規則(EU) 2016/679 の第 9 条第 1 項の適用において、法執行以外の目的のためのリモート生体要素識別の利用は、国内データ保護当局による禁止決定に既に服している。

Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, should continue to comply with all requirements resulting from Article 10 of Directive (EU) 2016/680. For purposes other than law enforcement, Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data subject to limited exceptions as provided in those Articles. In the application of Article 9(1) of Regulation (EU) 2016/679, the use of remote biometric identification for purposes other than law enforcement has already been subject to prohibition decisions by national data protection authorities.

- (40) TEU 及び TFEU に附属する自由、保安及び法務の領域に関する連合王国及びアイルランドの地位に関する議定書第 21 号の第 6 条 a に従い、アイルランドは、刑事における警察協力及び法務上の協力の分野における活動のための生体要素類型への振分けシステムの利用に対して同議定書が適用される範囲内において、この規則の第 5 条第 1 項第 1 副項(g)に定める規定によって拘束されず、この規則の第 5 条第 1 項第 1 副項(d)の適用のある AI システムの利用に対して同議定書が適用される範囲内において、同条項によって拘束されず、TFEU の第 16 条を基礎として定められた条項の遵守を要求する刑事における法務上の協力または警察協力の方式を規律する規定によってアイルランドが拘束されない場合、TFEU の第 3 部第 V 款の第 4 章または第 5 章の適用範囲内にある活動を実施する際における構成国による個人データの処理と関連する TFEU の第 16 条を基礎として採択されたこの規則の第 5 条第 1 項第 1 副項(h)、第 5 条第 2 項ないし第 6 項及び第 26 条第 10 項によって拘束されない。

In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph,

point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), Article 5(2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

- (41) TEU 及び TFEU に附属するデンマークの地位に関する議定書第 22 号の第 2 条及び第 2 条 a に従い、デンマークは、刑事における警察協力及び法務上の協力の分野における活動のための生体要素類型への振分けシステムの利用に対して同議定書が適用される範囲内において、この規則の第 5 条第 1 項第 1 副項(g)に定める規定によって拘束されず、この規則の第 5 条第 1 項第 1 副項(d)の適用のある AI システムの利用に対して同議定書が適用される範囲内において、同条項によって拘束されず、TFEU の第 3 部第 V 款の第 4 章または第 5 章の適用範囲内にある活動を実施する際における構成国による個人データの処理と関連する TFEU の第 16 条を基礎として採択されたこの規則の第 5 条第 1 項第 1 副項(h)、第 5 条第 2 項ないし第 6 項及び第 26 条第 10 項によって拘束されず、または、それらの条項の適用に服する。

In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not bound by rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), (2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

- (42) 無罪の推定に沿って、欧州連合内の自然人は、常に、当該自然人の実際の行動に関して裁判されるべきである。自然人は、客観的に検証可能な事実を基礎として当該個人が犯罪活動に関与しているという合理的な疑いなしに、かつ、その疑いに対する人間による評価なしに、国籍、出生地、居住地、子供の数、負債の程度、自動車の型式のような、当該個人のプロファイリング、人格特性または個性のみを基礎として、AI による予測行動に関し裁判されることがあってはならない。それゆえ、自然人の侵害行為の蓋然性を評価するため、または、現実の犯罪行為もしくは潜在的な犯罪行為の発生を予測するために、当該自然人をプロファイリングすることのみを基礎とし、または、当該自然人の人格特性及び個性を評価することのみを基礎として、自然人と関連して実施されるリスク評価は、禁止されるべきである。いかなる場合においても、この禁止は、疑いのある取引を基礎として事業者による粉飾の蓋然性を評価するためのリスク分析を用いる AI システムのような、または、例えば、既知の密輸経路を基礎として麻薬もしくは違法な物品の所在地である蓋然性を税関当局が推測するためのリスク分析ツールを用いる AI システムのような、個人のプロファイリングを基礎としないリスク分析または個人の人格特性もしくは個性を基礎としないリスク分析を指すものではなく、または、それに触れるものでもない。

In line with the presumption of innocence, natural persons in the Union should always be judged on their actual behaviour. Natural persons should never be judged on AI-predicted behaviour based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of debt or type of car, without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof. Therefore, risk assessments carried out with regard to natural persons in order to assess the likelihood of their offending or to predict the occurrence of an actual or potential criminal offence based solely on profiling them or on assessing their personality traits and characteristics should be prohibited. In any case, that prohibition does not refer to or touch upon risk analytics that are not based on the profiling of individuals or on the personality traits and characteristics of individuals, such as AI systems using risk analytics to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes.

- (43) インターネットまたは CCTV 映像記録からの顔画像の無差別的な要素抽出によって顔認識データベースを生成または拡張する AI システムを市場に置くこと、当該特別の目的のためにサービスに供すること、または、それを利用することは、その実務が大規模監視の気分を付加し、かつ、プライバシーの権利を含め、基本的な権利の総体的な侵害を導き得ることから、禁止されるべきである。

The placing on the market, the putting into service for **that specific purpose**, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, should be prohibited because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy.

- (44) とりわけ、文化と状況の全体を通じて、また、単独の個人の範囲内においてさえ、感情表現には大きな差異があるので、感情を識別または推論することを狙いとする AI システムの科学上の根拠に関しては、重大な懸念が存在する。その中でも、そのようなシステムの主たる欠点は、限定された信頼性、個別性の欠如及び限定された一般化能力である。それゆえ、当該自然人の生体要素データを基礎として自然人の感情または意図を識別または推論する AI システムは、差別的な成果を導き得るのであり、また、関係する個人の権利及び自由に対して侵害的であり得る。それらのシステムの侵害的な性質と併せて、労働または教育の過程における力の不均衡を考えると、そのようなシステムは、一定の自然人に対しまたは当該自然人のグループ全体に対し、差別的または好ましくない取扱いを導き得る。それゆえ、就労場所及び教育と関連する状況において個人の感情の状態を検出するために利用されることを意図する AI システムを市場に置くこと、サービスに供すること、または、利用することは、禁止されるべきである。この禁止は、治療上の利用を意図するシステムのような、厳格に医療上の理由または安全上の理由により市場に置かれる AI システムを包摂してはならない。

There are serious concerns about the scientific basis of AI systems aiming to identify or infer emotions, particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such systems are the limited reliability, the lack of specificity and the limited generalisability. Therefore, AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data may lead to discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons.

Considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof. Therefore, the placing on the market, the putting into service, or the use of AI systems intended to be used to detect the emotional state of individuals in situations related to the workplace and education should be prohibited. That prohibition should not cover AI systems placed on the market strictly for medical or safety reasons, such as systems intended for therapeutic use.

- (45) データ保護法, 差別禁止法, 消費者保護法及び競争法を含め, 欧州連合法によって禁止されている実務は, この規則によって影響を受けてはならない。

Practices that are prohibited by Union law, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation.

- (46) 高リスク AI システムは, 当該 AI システムが一定の強行的な要件を遵守している場合に限り, 欧州連合の市場に置かれ, サービスに供されまたは利用されるべきである。それらの要件は, 欧州連合内で利用可能な高リスク AI システムが, または, 欧州連合内において利用されるのではないとしても当該 AI システムの出力が, 欧州連合法によって認められかつ保護されている欧州連合の重要な公共の利益に対して許容できないリスクを呈さないことを確保すべきである。「EU の製品規定の実装に関する委員会告示『ブルーガイド』²⁰」の中で明確にされているような新たな立法枠組みのアプローチを基礎として, 適用可能な全ての欧州連合整合化立法を当該製品が遵守している場合に限り利用できるようにされることまたはサービスに供されることが生じ得ることから, 欧州議会及び理事会の規則(EU) 2017/745²¹及び規則(EU) 2017/746²²または欧州議会及び理事会の指令 2006/42/EC²³のような, 欧州連合整合化立法の複数の法行為が 1 個の製品に対して適用可能であり得ることが一般原則である。一貫性を確保するため, そして, 無用の行政上の負担と費用を避けるため, 1 または複数の高リスク AI システムを含んでおり, 当該製品に対してこの規則の要件及びこの規則の別紙中に列挙する欧州連合整合化立法の要件が適用される製品の提供者は, 1 または複数の AI システムを含む製

²⁰ OJ C 247, 29.6.2022, p. 1.

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

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

²² 体外診断用医療機器に関する並びに指令 98/79/EC 及び委員会決定 2010/227/EU を廃止する欧州議会及び理事会の 2017 年 4 月 5 日の規則(EU) 2017/746 (OJ L 117, 5.5.2017, p. 176).

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

²³ 機械に関する及び指令 95/16/EC を改正する欧州議会及び理事会の 2006 年 5 月 17 日の指令 2006/42/EC (OJ L 157, 9.6.2006, p. 24).

Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24).

品が欧州連合整合化立法の全ての適用可能な要件を最適な態様で遵守することをどのようにして確保するかに関する業務運営上の判断に関し、柔軟性をもつべきである。高リスクとして識別される AI システムは、欧州連合内の個人の健康、安全及び基本的な権利に対して大きく危険な影響をもつシステムに限定されるべきであり、また、そのような限定は、国際取引に対する潜在的な抑制を最小化すべきである。

High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. On the basis of the New Legislative Framework, as clarified in the Commission notice ‘The “Blue Guide” on the implementation of EU product rules 2022’⁽²¹⁾, the general rule is that more than one legal act of Union harmonisation legislation, such as Regulations (EU) 2017/745⁽²¹⁾ and (EU) 2017/746⁽²²⁾ of the European Parliament and of the Council or Directive 2006/42/EC of the European Parliament and of the Council⁽²³⁾, may be applicable to one product, since the making available or putting into service can take place only when the product complies with all applicable Union harmonisation legislation. To ensure consistency and avoid unnecessary administrative burdens or costs, providers of a product that contains one or more high-risk AI systems, to which the requirements of this Regulation and of the Union harmonisation legislation listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all applicable requirements of the Union harmonisation legislation in an optimal manner. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation should minimise any potential restriction to international trade.

- (47) AI システムは、とりわけ、そのようなシステムが製品の安全性コンポーネントとして機能する場合においては、個人の健康及び安全に対する負の影響をもち得る。域内市場における製品の支障のない移動を容易にするための、そして、安全な製品及びそれ以外の要件を遵守する製品のみが市場への道を見出すことを確保するための欧州連合整合化立法の諸目的と一貫性があり、AI システムを含め、当該製品のデジタルコンポーネントのゆえに全体としての製品によって生成され得る安全性のリスクが適正に防止及び緩和されることが重要である。例えば、製造業の過程においてであるか人の補助及び介助の過程においてであるかを問わず、自律性を増しているロボットは、複雑な環境の中で当該ロボットの機能を安全に運用及び遂行できるべきである。同様に、生命及び健康との関係の割合が特に高い医療部門においては、洗練度を増している診療システム及び人間の判断を支援するシステムは、信頼性があり、かつ、正確であるべきである。

AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and perform

their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate.

- (48) 憲章によって保護されている基本的な権利に対する AI システムから生ずる負の影響の範囲は、AI システムを高リスクとして分類する際、特に関連性をもつ。それらの権利は、人間の尊厳、私生活及び家庭の生活の尊重、個人データの保護、表現及び情報伝達の自由、集会及び団体の自由の権利、非差別の権利、教育の権利、消費者保護、労働者の権利、障害のある者の権利、ジェンダーの平等、知的財産権、実効的な救済及び公正な裁判の権利、防御の権利及び無罪の推定、良い行政の権利を含む。これらの諸権利に加え、憲章の第 24 条及び児童の権利に関する国際連合条約に掲げられ、デジタル環境と関連して UNCRC 一般見解第 25 号の中で更に発展させられた細目的な権利を児童がもっているということ、それら両者が児童の脆弱性に配慮すること及び児童の良い状態のために必要となるような保護と介助を提供することを要求していることを強調することが重要である。憲章の中に掲げられ、欧州連合の諸政策の中に実装された高いレベルの環境保護の基本的な権利もまた、個人の健康及び安全との関係を含め、AI システムが生じさせ得る危険の深刻度を評価する際、考慮に入れられるべきである。

The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, the right to education, consumer protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, and the right to good administration. In addition to those rights, it is important to highlight the fact that children have specific rights as enshrined in Article 24 of the Charter and in the United Nations Convention on the Rights of the Child, further developed in the UNCRC General Comment No 25 as regards the digital environment, both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons.

- (49) 製品もしくはシステムの安全性コンポーネントである高リスク AI システム、または、欧州議会及び理事会の規則(EC) No 300/2008²⁴、欧州議会及び理事会の規則(EU) No 167/2013²⁵、欧州議会及び理事会

²⁴ 民間航空の安全性の分野における共通規定に関する、及び、規則(EC) No 2320/2002 を廃止する欧州議会及び理事会の 2008 年 3 月 11 日の規則(EC) No 300/2008 (OJ L 97, 9.4.2008, p. 72).

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

²⁵ 農業車両及び林業車両の承認及び市場監視に関する欧州議会及び理事会の 2013 年 2 月 5 日の規則(EU) No 167/2013 (OJ L 60, 2.3.2013, p. 1).

Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).

の規則(EU) No 168/2013²⁶, 欧州議会及び理事会の指令 2014/90/EU²⁷, 欧州議会及び理事会の指令 (EU) 2016/797²⁸, 欧州議会及び理事会の規則(EU) 2018/858²⁹, 欧州議会及び理事会の規則(EU) 2018/1139³⁰並びに欧州議会及び理事会の規則(EU) 2019/2144³¹の適用範囲内にあり, それ自体が製

²⁶ 2 輪または 3 輪の車両及び 4 輪自転車の承認及び市場監視に関する欧州議会及び理事会の 2013 年 1 月 15 日の規則(EU) No 168/2013 (OJ L 60, 2.3.2013, p. 52).

Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

²⁷ 船舶用機器に関する及び理事会指令 96/98/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の指令 2014/90/EU (OJ L 257, 28.8.2014, p. 146).

Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

²⁸ 欧州連合内の鉄道システムの相互運用性に関する欧州議会及び理事会の 2016 年 5 月 11 日の指令(EU) 2016/797 (OJ L 138, 26.5.2016, p. 44).

Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).

²⁹ 自動車及びその被牽引車, そのような車両向けを意図したシステム, コンポーネント及びセパレート技術ユニットの承認及び市場監視に関する, 規則(EC) No 175/2007 及び規則(EC) No 595/2009 を改正する, 並びに, 指令 2007/46/EC を廃止する欧州議会及び理事会の 2018 年 5 月 30 日の規則(EU) 2018/858 (OJ L 151, 14.6.2018, p. 1).

Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

³⁰ 民間航空の分野における共通規定に関する, 及び, 欧州連合航空安全局を設置する, 並びに, 欧州議会及び理事会の規則(EC) No 2111/2005, 規則(EC) No 1008/2008, 規則(EU) No 996/2010, 規則(EU) No 376/2014, 指令 2014/30/EU 及び指令 2014/53/EU を改正する, 並びに, 欧州議会及び理事会の規則(EC) No 552/2004, 規則(EC) No 216/2008 及び理事会規則(EEC) No 3922/91 を廃止する欧州議会及び理事会の 2018 年 7 月 4 日の規則(EU) 2018/1139 (OJ L 212, 22.8.2018, p. 1).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

³¹ 自動車及びその被牽引車の一般的な安全性並びに車両乗員及び脆弱な道路利用者の保護と関連して, そのような車両, そのような車両向けを意図したシステム, コンポーネント及びセパレート技術ユニットの型式承認の要件に関する, 欧州議会及び理事会の規則(EU) 2018/858 を改正する, 欧州議会及び理事会の規則(EC) No 78/2009, 規則(EC) No 79/2009 及び規則(EC) No 661/2009 並びに委員会規則(EC) No 631/2009, 委員会規則(EU) No 406/2010, 委員会規則(EU) No 672/2010, 委員会規則(EU) No 1003/2010, 委員会規則(EU) No 1005/2010, 委員会規則(EU) No 1008/2010, 委員会規則(EU) No 1009/2010, 委員会規則(EU) No 19/2011, 委員会規則(EU) No 109/2011, 委員会規則(EU) No 458/2011, 委員会規則(EU) No 65/2012, 委員会規則(EU) No 130/2012, 委員会規則(EU) No 347/2012, 委員会規則(EU) No 351/2012, 委員会規則(EU) No 1230/2012 及び委員会規則(EU) 2015/166 を廃止する欧州議会及び理事会の 2019 年 11 月 27 日の規則(EU) 2019/2144 (OJ L 325, 16.12.2019, p. 1).

Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No

品もしくはシステムである高リスク AI システムに関しては、これらの法行為を基礎とする委任される行為または実装行為を採択する際、個々の部門の技術上及び法制上の特性を基礎とし、かつ、現行の統治、適合性評価及び執行の仕組み並びにこれらの仕組み内に設けられた機関に対して干渉することなく、この規則の中で定められた高リスク AI システムの強行的な要件を欧州委員会が考慮に入れることを確保するため、それらの法行為を改正することが適切である。

As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council ⁽²⁴⁾, Regulation (EU) No 167/2013 of the European Parliament and of the Council ⁽²⁵⁾, Regulation (EU) No 168/2013 of the European Parliament and of the Council ⁽²⁶⁾, Directive 2014/90/EU of the European Parliament and of the Council ⁽²⁷⁾, Directive (EU) 2016/797 of the European Parliament and of the Council ⁽²⁸⁾, Regulation (EU) 2018/858 of the European Parliament and of the Council ⁽²⁹⁾, Regulation (EU) 2018/1139 of the European Parliament and of the Council ⁽³⁰⁾ and Regulation (EU) 2019/2144 of the European Parliament and of the Council ⁽³¹⁾, it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant delegated or implementing acts on the basis of those acts.

- (50) 製品の安全性コンポーネントである AI システムまたはそれ自体が製品である AI システムであって、この規則の別紙の中に列挙される一定の欧州連合整合化立法の適用範囲内にあるものに関しては、関係する製品が、関連する欧州連合整合化立法による第三者適合性評価組織の適合性評価手続を実施するときは、この規則の下において高リスクとしてそのシステムを分類することが適切である。とりわけ、機械、玩具、昇降機、潜在的に爆発の危険性のある状態における利用を意図する機器及び防護システム、無線機器、加圧機器、娯楽用船舶機器、ロープウェイ設備、気化燃料を燃焼する器具、医療機器、体外診断用医療機器、自動車及び航空機は、そのような製品である。

As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain Union harmonisation legislation listed in an annex to this Regulation, it is appropriate to classify them as high-risk under this Regulation if **the product concerned undergoes** the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, in vitro diagnostic medical devices, automotive and aviation.

- (51) この規則による高リスクとしての AI システムの分類は、関連する欧州連合整合化立法の中で設けられた当該製品に適用される基準の下において、当該製品の安全性コンポーネントが AI システムで

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 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

ある製品またはそれ自身が製品である AI システムが、高リスクであると判断されることを必ずしも意味すべきではない。とりわけ、中リスク製品及び高リスク製品に関する第三者適合性評価が定められている規則(EU)2017/745 並びに規則(EU)2017/746 がその場合である。

The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered to be high-risk under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is, in particular, the case for Regulations (EU) 2017/745 and (EU) 2017/746, where a third-party conformity assessment is provided for medium-risk and high-risk products.

- (52) スタンドアロンの AI システム、すなわち、製品の安全性コンポーネントである AI システムまたはそれ自身が製品である AI システム以外の高リスク AI システムに関しては、当該 AI システムの所期の目的に照らし、あり得る危険の深刻度及び当該危険の発生の蓋然性の両者を考慮に入れた上で、健康及び安全または個人の基本的な権利に対する危険の高いリスクをそのシステムが呈しており、かつ、この規則の中で細目が定められた多数の個別の事前定義された分野においてそのシステムが利用されるときは、その AI システムを高リスクとして分類することが適切である。それらの AI システムの識別は、高リスク AI システムのリストの将来の改正のためにも予定されている同じ手法及び基準を基礎としており、欧州委員会は、技術開発の急速なペースと AI システムの利用における潜在的な変化を考慮に入れるため、委任される行為を介して、採択する権限を与えられるべきである。

As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems that the Commission should be empowered to adopt, via delegated acts, to take into account the rapid pace of technological development, as well as the potential changes in the use of AI systems.

- (53) 当該 AI システムが意思決定に対して実質的に影響を与えないという理由、または、当該適法な利益に対して実質的に危険を及ぼさないという理由により、この規則の中で細目が定められる事前定義された分野の中で示される AI システムが、それらの分野の下において保護されている適法な利益に対する危険の重大なリスクを導かない個別の場合があり得るということを明確にすることも重要である。この規則の目的のために、意思決定の結果に対して実質的に影響を与えない AI システムとは、人間の意思決定であるか自動化された意思決定であるかを問わず、その内容に対する影響をもち、それゆえ意思決定の結果に対して影響をもちない AI システムであると理解されるべきである。意思決定の結果に対して実質的に影響を与えない AI システムは、当該状況内において以下の 1 または複数の条件が満たされている状況を含み得る。そのような第 1 の条件は、構造化されていないデータを構造化されたデータへと変換する AI システム、受領した文書を類型毎に振分ける AI システムまたは多数の申込の中の重複を検出するために利用される AI システムのような、ごく狭い手

継続的な仕事を遂行することをその AI システムが意図していることであるべきである。それらの仕事は、この規則の別紙中に高リスクな利用として列挙される過程における AI システムの利用を通じて増加されることのない限定的なリスクのみを呈するような、ごく狭い限定的な性質のものである。第 2 の条件は、この規則の別紙中に列挙される高リスクな利用の目的のために適合したものであり得る事前に完了した人間の活動の結果を改善することをその AI システムによって遂行される仕事が意図していることであるべきである。それらの高リスクの利用の特性を考えると、その AI システムは、人間の活動に対して、結果的に低められたリスクをもつ付加的なレイヤを提供するだけである。例えば、この条件は、例えば、専門家の言い回し、学術的な言語スタイルとの関係において、または、あるブランドのメッセージングに文を揃えることによって、事前に作成された文書に使用される言語を改善することを意図する AI システムに対して適用されることだろう。第 3 の条件は、意思決定パターンを検出することまたは従前の意思決定パターンからの逸脱を検出することをその AI システムが意図していることであるべきである。その AI システムの利用が事前に完了した人間による評価後であり、それは、人間による適切な見直しのない置換えや影響を意味しないことから、そのリスクは、低められるだろう。そのような AI システムは、例えば、教員の一定の成績評価パターンに鑑み、潜在的な一貫性喪失または異常にフラグを立てるため、その教員がその成績評価パターンから逸脱したか否かを事後的に検査するために利用され得る AI システムを含む。第 4 の条件は、この規則の別紙の中に列挙される AI システムの目的のために適合した評価を準備することだけ、そして、従うべき評価のためのリスクが現れという面において当該システムの出力のあり得る影響を非常に低くするという仕事を遂行することをその AI システムが意図していることであるべきである。この条件は、就中、索引付け、検索、文と発話の処理もしくは別のデータ源への結びつけからの様々な機能を含むファイル取扱いのためのスマートリビューションに対し、または、元の文書の翻訳のために利用される AI システムに対し適用される。いずれの場合においても、この規則の別紙中に列挙される高リスク利用の場合に利用される AI システムは、その AI システムが、規則(EU) 2016/679 の第 4 条第 4 号または指令(EU) 2016/680 の第 3 条第 4 号または規則(EU) 2018/1725 の第 3 条第 5 号の意味におけるプロファイリングを含意するときは、健康、安全または基本的な権利に対する危険の大きなリスクを呈すると判断されるべきである。追跡可能性と透明性を確保するため、上記に示した諸条件を基礎として、AI システムが高リスクではないと判断する提供者は、当該システムが市場に置かれまたはサービスに供される前に評価の文書を作成すべきであり、また、求めに応じて、職務権限のある国内当局に対し、その文書を提供すべきである。そのような提供者は、この規則の下において設けられる EU データベースにその AI システムを登録することを義務づけられるべきである。この規則の別紙の中に列挙される AI システムが例外的に非高リスクであることの基礎となる諸条件の実務上の実装のために別の指針を提供するという観点から、欧州委員会は、委員会から意見聴取をした後、その実務上の実装の細目を定め、高リスク AI システムの利用例と非高リスク AI システムの利用例の実例の包括的なリストを網羅する指針を提供する。

It is also important to clarify that there may be specific cases in which AI systems referred to in pre-defined areas specified in this Regulation do not lead to a significant risk of harm to the legal interests protected under those areas because they do not materially influence the decision-making or do not harm those interests substantially. For the purposes of this Regulation, an AI system that does not materially influence the outcome of decision-making should be understood to be an AI system that does not have an impact on the substance, and thereby the outcome, of decision-

making, whether human or automated. An AI system that does not materially influence the outcome of decision-making could include situations in which one or more of the following conditions are fulfilled. The first such condition should be that the AI system is intended to perform a narrow procedural task, such as an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories or an AI system that is used to detect duplicates among a large number of applications. Those tasks are of such narrow and limited nature that they pose only limited risks which are not increased through the use of an AI system in a context that is listed as a high-risk use in an annex to this Regulation. The second condition should be that the task performed by the AI system is intended to improve the result of a previously completed human activity that may be relevant for the purposes of the high-risk uses listed in an annex to this Regulation. Considering those characteristics, the AI system provides only an additional layer to a human activity with consequently lowered risk. That condition would, for example, apply to AI systems that are intended to improve the language used in previously drafted documents, for example in relation to professional tone, academic style of language or by aligning text to a certain brand messaging. The third condition should be that the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns. The risk would be lowered because the use of the AI system follows a previously completed human assessment which it is not meant to replace or influence, without proper human review. Such AI systems include for instance those that, given a certain grading pattern of a teacher, can be used to check *ex post* whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies. The fourth condition should be that the AI system is intended to perform a task that is only preparatory to an assessment relevant for the purposes of the AI systems listed in an annex to this Regulation, thus making the possible impact of the output of the system very low in terms of representing a risk for the assessment to follow. That condition covers, *inter alia*, smart solutions for file handling, which include various functions from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents. In any case, AI systems used in high-risk **use-cases** listed in an annex to this Regulation should be considered to pose significant risks of harm to the health, safety or fundamental rights if the AI system implies profiling within the meaning of Article 4, point (4) of Regulation (EU) 2016/679 or Article 3, point (4) of Directive (EU) 2016/680 or Article 3, point (5) of Regulation (EU) 2018/1725. To ensure traceability and transparency, a provider who considers that **an AI system** is not high-risk on the basis of the conditions referred to above should draw up documentation of the assessment before that system is placed on the market or put into service and should provide that documentation to national competent authorities upon request. Such a provider should be obliged to register the AI system in the EU database established under this Regulation. With a view to providing further guidance for the practical implementation of the conditions under which the AI systems listed in an annex to this Regulation are, on an exceptional basis, non-high-risk, the Commission should, after consulting the Board, provide guidelines specifying that practical implementation, completed by a comprehensive list of practical examples of use cases of AI systems that are high-risk and use cases that are not.

- (54) 生体要素データは特別類型の個人データを組成するので、関連する欧州連合法及び国内法の下において当該個人データの利用が許容される限り、生体要素システムの幾つかの高リスクの重要な利用例として分類することが適切である。自然人のリモート生体要素識別を意図する AI システムの技術上の不正確性は、バイアスのかかった結果を導き得るのであり、かつ、差別的な効果を伴う。そのようなバイアスのかかった結果及び差別的な効果のリスクは、年齢、民族、人種、性または障害と関連して特に適合性がある。それゆえ、リモート生体要素識別システムは、それらのシステムが呈す

るリスクを考慮し、高リスクとして分類されるべきである。そのような分類は、認証を含め、生体要素の検証のために利用されることを意図する AI システムであって、ある特定の自然人が、当該の者がその者であると主張する者であることを確認することのみをその AI システムの目的とするもの、及び、あるサービスへのアクセスをもつこと、機器のロックを解除することまたは施設へのセキュリティアクセスをもつことという目的のみのために自然人の同一性を確認することのみをそのシステムの単独の目的とするものを除外する。加えて、この規則の下においてそれらの AI システムが禁止されていない限り、生体要素データを基礎とし、規則(EU) 2016/679 の第 9 条第 1 項の下において保護される機微の属性または特性に従って生体要素類型への振分けのために利用されることを意図する AI システム、並びに、この規則の下において禁止されていない感情認識システムは、高リスクとして分類されるべきである。サイバーセキュリティ及び個人データ保護の方策を実現できるようにする目的のみのため利用されることを意図する生体要素システムは、高リスク AI システムとして判断されてはならない。

As biometric data constitutes a special category of personal data, it is appropriate to classify as high-risk several critical-use cases of biometric systems, insofar as their use is permitted under relevant Union and national law. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. The risk of such biased results and discriminatory effects is particularly relevant with regard to age, ethnicity, race, sex or disabilities. Remote biometric identification systems should therefore be classified as high-risk in view of the risks that they pose. Such a classification excludes AI systems intended to be used for biometric verification, including authentication, the sole purpose of which is to confirm that a specific natural person is who that person claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having secure access to premises. In addition, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics protected under Article 9(1) of Regulation (EU) 2016/679 on the basis of biometric data, in so far as these are not prohibited under this Regulation, and emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk. Biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures should not be considered to be high-risk AI systems.

- (55) 不可欠なインフラの運営管理及び運用に関しては、当該 AI システムの不良または誤作動が個人の生命及び健康を大規模にリスクに晒し得るので、また、社会活動及び経済活動を正常に行う上での大混乱を導き得るので、指令(EU) 2022/2557 の別紙の第 8 号に列挙する不可欠のデジタルインフラ、道路交通並びに水、ガス、暖房及び電気の供給の運営管理及び運用における安全性コンポーネントとして利用されることを意図する AI システムを高リスクとして分類することが適切である。不可欠デジタルインフラを含め、不可欠インフラの安全性コンポーネントは、不可欠インフラの物理的な完全性または個人の健康及び安全並びに財産を直接に保護するために利用されるシステムであるが、それは、システムが稼働するためのものであるとは限らない。そのようなコンポーネントの不良または誤作動は、不可欠インフラの物理的な完全性に対するリスク、そして、個人の健康及び安全並びに財産に対するリスクを直接に導き得る。サイバーセキュリティ上の目的のためにのみ利用されることを意図するコンポーネントは、安全性コンポーネントとして分類されてはならない。そのような不可欠インフラの安全性コンポーネントの例は、水圧を監視するためのシステムまたはクラウドコンピューティングセンター内の火災警報管理システムを含み得る。

As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of critical digital infrastructure as listed in point (8) of the Annex to Directive (EU) 2022/2557, road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. Safety components of critical infrastructure, including critical digital infrastructure, are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of persons and property but which are not necessary in order for the system to function. The failure or malfunctioning of such components might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property. Components intended to be used solely for cybersecurity purposes should not qualify as safety components. Examples of safety components of such critical infrastructure may include systems for monitoring water pressure or fire alarm controlling systems in cloud computing centres.

- (56) 教育における AI システムの設置は、高品位のデジタル教育及び訓練を促進するために重要であり、また、メディアリテラシ及び批判的な思考を含め、経済、社会において及び民主的な過程において積極的な役割を演ずるために必要となるデジタルの技能と能力を全ての学習者と教員が獲得及び共有できるようにするために重要である。ただし、とりわけ、アクセスもしくは入学の判定のため、全てのレベルの教育及び職業訓練の機関または計画へ個人を振分けるため、個人の学習成果の評価のため、個人のための適切な教育レベルを評価するため、並びに、個人が受けることになるもしくはアクセスできるようになる教育と訓練のレベルに対して実質的に影響を与えるため、または、試験の間における生徒の禁止された行動の監視及び検知のため、教育または職業訓練において利用される AI システムは、個人の生涯の教育課程及び職業課程をそれらの AI システムが決定し得るものであり、それゆえ、生活を安全にするための個人の能力に対して影響を与え得るものであるため、高リスク AI システムとして分類されるべきである。不適切に設計され及び利用される場合、そのようなシステムは、とりわけ侵害的であり得るのであり、かつ、教育及び訓練の権利並びに差別に対して反対する権利を侵害し得るのであり、そして、例えば、女性、一定の年齢のグループ、障害をもつ人々、または、一定の人種もしくは民族的な出自の人々、または、一定の性的指向をもつ人々にとって不利に、歴史的な差別パターンを永続化させる。

The deployment of AI systems in education is important to promote high-quality digital education and training and to allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes. However, AI systems used in education or vocational training, in particular for determining access or admission, for assigning persons to educational and vocational training institutions or programmes at all levels, for evaluating learning outcomes of persons, for assessing the appropriate level of education for an individual and materially influencing the level of education and training that individuals will receive or will be able to access or for monitoring and detecting prohibited behaviour of students during tests should be classified as high-risk AI systems, since they may determine the educational and professional course of a person's life and therefore may affect that person's ability to secure a livelihood. When improperly designed and used, such systems may be particularly intrusive and may violate the right to education and training as well as the right not to be discriminated against and **perpetuate** historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or

sexual orientation.

- (57) 特に、個人の採用と選抜のため、仕事と関連する関係をもつ期間、昇進及び仕事と関連する契約関係の終了に影響を与える判断を行うため、個人の行動、個人の特性もしくは個性を基礎として仕事を割当てるため、並びに、仕事関連の契約関係において個人を監視または評価するために、雇用、労働者の管理及び自営へのアクセスにおいて利用される AI システムもまた、当該の者の将来のキャリアの見通しと生活及び労働者の権利に対してそれらのシステムがかなりの影響をもち得るので、高リスクとして分類されるべきである。適合する仕事関連の契約関係は、欧州委員会の 2021 年作業計画の中に示されているプラットフォームを通じてサービスを提供する従業者及び個人を、意味のある態様で含めるべきである。採用過程全体を通じて、及び、仕事関連の契約関係における個人の評価、昇進または人材確保において、そのようなシステムは、例えば、女性、一定の年齢のグループ、障害をもつ人々、または、一定の人種もしくは民族的な出自の人々、または、一定の性的指向をもつ人々にとって不利に、歴史的な差別パターンを永続化させ得る。そのような個人の遂行能力及び行動を監視するために利用される AI システムもまた、当該個人のデータ保護及びプライバシーの基本的な権利を損ね得る。

AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Relevant work-related contractual relationships should, in a meaningful manner, involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to data protection and privacy.

- (58) AI システムの利用が特に考慮されているもう 1 つの分野は、社会への全面的な参加のためまたは人の生活水準を向上させるために人々にとって必要な民間及び公共の一定の必須サービスと受給へのアクセスとその享受である。とりわけ、行政機関からの必須の公共補助、すなわち、医療サービス、社会保険の受給、妊娠、疾病、労働災害、要介護または老齢及び失業のような場合における保護を提供する社会サービス並びに社会補助及び住宅補助の受給と役務提供を申請している自然人またはそれらを受給している自然人は、典型的に、それらの受給と役務提供に依存しており、かつ、職責のある当局との関係において脆弱な立場にある。受給者がそのような受給または役務提供を受ける適法な資格をもつかどうかを含め、そのような受給及び役務提供が当局から認められ、拒否され、減額され、取消されまたは返還請求されるべきかどうかを判定するために AI システムが利用される場合、そのシステムは、個人の生活に対して大きな影響をもち得るのであり、また、社会的保護、非差別、人間の尊厳または実効的な救済の権利のような当該個人の基本的な権利を侵害し得るので

あり、それゆえ、高リスクとして分類されるべきである。ただし、この規則は、当該 AI システムが法人及び自然人する高リスクを伴わないことを条件として、法令を遵守する安全な AI システムのより広範な利用からの受益に資するような行政機関における革新的なアプローチの開発及び利用を妨げてはならない。加えて、自然人の信用度または与信限度額を評価するために利用される AI システムは、資金源または住宅、電気及び電話のサービスのような必須サービスへの当該個人のアクセスをそのシステムが判定するので、高リスク AI システムとして分類されるべきである。それらの目的のために利用される AI システムは、個人またはグループの間における差別を導き得るものであり、また、例えば、人種的または民族的な出自、ジェンダー、障害、年齢、性的指向を基礎とする差別のような歴史的な差別パターンを永続化させ得るものであり、または、新たな形態の差別的な影響をつくり出し得る。ただし、金融サービスの提供における詐偽行為の検知の目的のため、及び、与信機関および保険事業者の資本要件を計算するための健全性の目的のために欧州連合法によって定められる AI システムは、この規則の下において高リスクとして判断されてはならない。それに加えて、健康保険及び生命保険を求める自然人と関係するリスク評価及び価格設定のために利用されることを意図する AI システムもまた、個人の生活に対して重大な影響をもち得るのであり、また、適正に設計され、開発され及び利用されていないときは、当該個人の基本的な権利を侵害し得るのであり、かつ、金融上の疎外及び差別を含め、人々の生活と健康にとって重大な結果を導き得る。最後に、自然人からの緊急電話を評価及び分類するために利用される AI システム、または、警察、消防及び救急医療による場合を含め、緊急初期対応サービス及び緊急医療患者トリアージシステムの発動において、発動のためもしくは優先順位を定めるために利用される AI システムもまた、個人の生命と健康及び当該個人の財産にとって極めて重要な状況下においてそのシステムが判定を行うので、高リスクとして分類されるべきである。

Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of **certain essential private and public services and benefits** necessary for people to fully participate in society or to improve one's standard of living. In particular, natural persons applying for or receiving essential public assistance benefits and services from public authorities namely healthcare services, social security benefits, social services providing protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment and social and housing assistance, are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be granted, denied, reduced, revoked or reclaimed by authorities, including whether beneficiaries are legitimately entitled to such benefits or services, those systems may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy and should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. In addition, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on **racial or ethnic origins**, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts. However, AI systems provided for by

Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation. Moreover, AI systems intended to be used for risk assessment and pricing in relation to natural persons for health and life insurance can also have a significant impact on persons' livelihood and if not duly designed, developed and used, can infringe their fundamental rights and can lead to serious consequences for people's life and health, including financial exclusion and discrimination. Finally, AI systems **used to evaluate and classify emergency calls by natural persons or to dispatch or establish** priority in the dispatching of emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems, should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

- (59) 法執行機関の役割及び職責に鑑み、法執行機関による AI システムの一定の利用を含む活動は、大きな度合いの力の不均衡によって特徴づけられ、かつ、監視、逮捕または自然人の自由の剥奪を導き得るものであり、また、憲章の中で保障された基本的な権利に対してそれら以外の負の影響を与え得る。とりわけ、その AI システムが高品質のデータによって訓練されておらず、そのシステムの性能、そのシステムの正確性またはその堅牢性の面において適切な要件に適合しておらず、または、適正に設計されておらず、かつ、市場に置かれる前に、もしくは、そうでなければサービスに供される前に試験されていないときは、そのシステムは、差別的な態様でまたは差別的ではないとしても不正確もしくは正当化されない態様で、人々を選別し得る。更に、とりわけ、そのような AI システムが、十分な透明性がなく、説明可能性がなく、かつ、文書化されていない場合、実効的な救済と公正な裁判の権利及び防御の権利と無罪の推定のような、重要な手続上の基本的な権利の行使が阻害され得る。それゆえ、負の影響を避けるため、公衆の信頼を維持するため、及び、説明責任と実効的な救済を確保するために正確性、信頼性及び透明性がとりわけ重要である法執行の過程において利用されることを意図する多数の AI システムは、関連する欧州連合法及び国内法の下においてそのシステムの利用が許容される限り、高リスクとして分類することが適切である。その活動の性質及びその活動と関連するリスクを考慮し、それらの高リスク AI システムは、とりわけ、犯罪行為の被害者となる自然人のリスクの評価のためにポリグラフ及びそれと類似のツールとして、犯罪行為の捜査もしくは訴追の過程における証拠の信頼性の評価のために、この規則の下において禁止されていない限り、自然人のプロファイリングのみを基礎とすることなく、犯罪行為を実行するもしくは再犯を実行する自然人のリスクを評価するため、または、自然人もしくはグループの人格特性及び個性もしくは過去の犯罪行為を評価するために、犯罪行為の検知、捜査もしくは訴追の過程におけるプロファイリングのために、法執行機関もしくはその代わりの者によって、または、法執行機関を支援する欧州連合の機関、組織、事務局もしくは部局によって、利用されることを意図する AI システムを含めるべきである。税務当局及び関税当局による行政手続のため、または、欧州連合の資金洗浄禁止法により情報を分析する行政上の職務を遂行する金融情報ユニットによる行政手続のために利用されることを特に意図する AI システムは、犯罪行為の防止、検知、捜査及び訴追の目的のために法執行機関によって利用される高リスク AI システムとして分類されてはならない。法執行機関及びそれ以外の関連当局による AI ツールの利用は、不平等または疎外の要素となってはならない。被疑者の防御の権利に対して AI ツールを利用することの影響、とりわけ、それらのシステムの稼働に関する意味のある情報を得る上での困難性、そして、その結果として、とりわけ犯罪捜査の下にある個人によって法廷においてそのシステムの結果に異議を述べるのが困難となることは、無視されてはならない。

Given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high-quality data, does not meet adequate requirements in terms of its performance, its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk, insofar as their use is permitted under relevant Union and national law, a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices, or agencies in support of law enforcement authorities for assessing the risk of a natural person to become a victim of criminal offences, as polygraphs and similar tools, for the evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences, and, insofar as not prohibited under this Regulation, for assessing the risk of a natural person offending or reoffending not solely on the basis of the profiling of natural persons or the assessment of personality traits and characteristics or the past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of prevention, detection, investigation and prosecution of criminal offences. The use of AI tools by law enforcement and other relevant authorities should not become a factor of inequality, or exclusion. The impact of the use of AI tools on the defence rights of suspects should not be ignored, in particular the difficulty in obtaining meaningful information on the functioning of those systems and the resulting difficulty in challenging their results in court, in particular by natural persons under investigation.

- (60) 移民、難民及び出入国管理において利用される AI システムは、しばしばとりわけ脆弱な立場にある人々及び職務権限のある行政機関の活動の結果に依存している人々に対し、影響を与える。それゆえ、それらの過程において利用される AI システムの正確性、非差別の性質及び透明性は、影響を受ける個人の基本的な権利、とりわけ、当該個人の支障のない移動、非差別、私生活及び個人データの保護、国際的な保護及び良い行政の権利の尊重を保障するため、とりわけ重要である。それゆえ、関連する欧州連合法及び国内法の下において当該 AI システムの利用が許容される限り、構成国の領土に入国する自然人または査証の申請もしくは難民の申請を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、それと関連する証拠の信頼性の評価を含め、難民、査証及び居住許可の申請、並びに、地位を求める申請をする自然人の適格性を認定するための目的と関係する関連不服申立ての審査に関して職務権限のある行政機関を補助するため、渡航文書の検査を除き、移民、難民及び出入国管理の過程において自然人を検知すること、認識することまたは識別することという目的のために、移民、難民及び出入国管理の分野における職務を遂行する職務権限のある

行政機関もしくはその代替りの者によって、または、欧州連合の機関、組織、事務局もしくは部局によって、ポリグラフ及びそれと類似のツールとして利用されることを意図する AI システムを高リスクとして分類することが適切である。この規則の適用のある移民、難民及び国境管理の分野における AI システムは、欧州議会及び理事会の規則(EC) No 810/2009³²、欧州議会及び理事会の指令 2013/32/EU³³並びにこれら以外の関連する欧州連合法によって定められた手続上の関連要件を遵守すべきである。移民、難民及び出入国管理における AI システムの利用は、いかなる状況においても、1967 年 1 月 31 日の議定書によって改正されたものとしての 1951 年 7 月 28 日にジュネーブにおいて行われた難民の地位に関する条約の下における構成国または欧州連合の機関、組織、事務局もしくは部局の国際的な義務を回避するための手段として、構成国または欧州連合の機関、組織、事務局もしくは部局によって利用されてはならない。また、当該 AI システムは、いかなる方法においても、ノン・フルマンの原則に違反するため、または、国際的な保護の権利を含め、欧州連合の領土内への安全かつ実効的な適法な移動を拒否するために利用されてはならない。

AI systems used in migration, asylum and border control management affect persons who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee respect for the fundamental rights of the affected persons, in particular their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk, insofar as their use is permitted under relevant Union and national law, AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools, for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum, for assisting competent public authorities for the examination, including related assessment of the reliability of evidence, of applications for asylum, visa and residence permits and associated complaints **with regard to the objective to establish the eligibility** of the natural persons applying for a status, for the purpose of detecting, recognising or identifying natural persons in the context of migration, asylum and border control management, with the exception of verification of travel documents. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Regulation (EC) No 810/2009 of the European Parliament and of the Council⁽³²⁾, the Directive 2013/32/EU of the European Parliament and of the Council⁽³³⁾, and other relevant Union law. The use of AI systems in migration, asylum and border control management should, in no circumstances, be used by Member States or Union institutions, bodies, offices or agencies as a means to circumvent their international obligations under the UN Convention relating to the Status of Refugees done at Geneva on 28 July 1951 as amended by the Protocol of 31 January 1967. Nor should they

³² 査証に関する欧州共同体法典を定める欧州議会及び理事会の 2009 年 7 月 13 日の規則(EC) No 810/2009 (Visaコード)(OJ L243, 15.9.2009, p. 1).

Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L243, 15.9.2009, p. 1).

³³ 国際的な保護の付与及び撤回のための共通手続に関する欧州議会及び理事会の 2013 年 6 月 26 日の指令 2013/32/EU(OJ L 180, 29.6.2013, p. 60).

Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

be used to in any way infringe on the principle of non-refoulement, or to deny safe and effective legal avenues into the territory of the Union, including the right to international protection.

- (61) 民主主義、法の支配、個人の自由並びに実効的な救済及び公正な裁判の権利に対する潜在的に重大な影響を考慮し、法務及び民主的な過程の運営を意図する一定の AI システムは、高リスクとして分類されるべきである。とりわけ、潜在的なバイアス、エラー及び不透明性のリスクに対処するため、事実及び法律の検索及び解釈において並びに具体的な事実のセットへの法律の適用において法務当局を補助するため、法務当局によってまたはその代わりにの者によって利用されることを意図する AI システムは、高リスクとして分類するのが適切である。それらの目的のために裁判外紛争解決組織によって利用されることを意図する AI システムもまた、その裁判外紛争解決手続の成果が当事者に対して法的効果を生成するときは、高リスクであると判断されるべきである。AI ツールの利用は、判事意思決定の権限または法務の独立を支援し得るが、それを置き換えてはならない。最終的な意思決定は、人間が調整する活動のままでなければならない。ただし、高リスクとしての AI システムの分類は、法務当局の判断、文書またはデータの匿名化または仮名化、関係者間の通信、行政上の職務のような、個々の事件における現実の法務上の行政に対して影響を与えることのない、純粋に補助的な行政活動を意図する AI システムに対して拡張してはならない。

Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, considering their potentially significant impact on democracy, the rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to be used by a judicial authority or on its behalf to assist judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts. AI systems intended to be used by alternative dispute resolution bodies for those purposes should also be considered to be high-risk when the outcomes of the alternative dispute resolution proceedings produce legal effects for the parties. The use of AI tools can support the decision-making power of judges or judicial independence, but should not replace it: the final decision-making must remain a human-driven activity. The classification of AI systems as high-risk should not, however, extend to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks.

欧州議会及び理事会の規則(EU) 2024/900³⁴に定める規定を妨げることなく、かつ、憲章の第 39 条に掲げられた投票の権利に対する不適切な外的影響のリスクに対処するため、及び、民主主義と法の支配に対する負の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対して影響を与えるまたは選挙もしくは国民投票において当該自然人の投票権を行使する自然人の投票行動に対して影響を与えるために利用されることを意図する AI システムは、運営及び物資管理の観点から政治

³⁴ 政治的な宣伝行為の透明性及びターゲティングに関する欧州議会及び理事会の 2024 年 3 月 13 日の規則 (EU) 2024/900 (OJL, 2024/900, 20.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/900/oj>).

Regulation (EU) 2024/900 of the European parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (OJL, 2024/900, 20.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/900/oj>).

的なキャンペーンを組織し、最適化し及び構造化するために利用されるツールのような、そのシステムの出力に対して自然人が直接に晒されることがない AI システムを除き、高リスク AI システムとして分類されるべきである。

Without prejudice to the rules provided for in Regulation (EU) 2024/900 of the European Parliament and of the Council⁽⁶⁴⁾, and in order to address the risks of undue external interference with the right to vote enshrined in Article 39 of the Charter, and of adverse effects on democracy and the rule of law, AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda should be classified as high-risk AI systems with the exception of AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistical point of view.

- (63) ある AI システムがこの規則の下において高リスク AI システムとして分類されたという事実は、個人データの保護に関するもの、自然人の感情の状態を検出するためのポリグラフ及びそれと類似のツールまたはそれら以外のシステムの利用に関するもののような、欧州連合法の他の法行為の下においてまたは欧州連合法と互換性のある国内法の下において、そのシステムの利用が適法であるということを示すものとして解釈されてはならない。そのような利用は、憲章から並びに欧州連合の二次法の適用可能な法行為及び国内法から帰結する適用可能な要件に従う場合に限り、生じ続けるべきである。この規則は、それが関連するときは、この規則の中で特に別異に定めていない限り、特別類型の個人データを含め、個人データの処理のための適法性の根拠を定めるものとして理解されてはならない。

The fact that an AI system is classified as a high-risk AI system under this Regulation should not be interpreted as indicating that the use of the system is lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant, unless it is specifically otherwise provided for in this Regulation.

- (64) 市場に置かれまたはサービスに供される高リスク AI システムからのリスクを緩和するため、及び、高いレベルの信頼性を確保するため、当該 AI システムの所期の目的及び利用の過程を考慮に入れた上で、かつ、その提供者によって設けられるリスク管理システムに従い、高リスク AI システムに対し、一定の強行的な要件が適用されるべきである。この規則の強行的な要件を遵守するために提供者によって採用される方策は、AI に関する一般に承認された最新技術を考慮に入れるべきであり、この規則の目的に適合するために比例的かつ実効的であるべきである。委員会告示「EU の製品規定の実装に関する『ブルーガイド』2022」の中で明確にされているような新たな立法枠組みのアプローチを基礎として、適用可能な全ての欧州連合整合化立法を当該製品が遵守している場合に限り利用できるよにされまたはサービスに供することが行われ得るので、1 個の製品に対して複数の欧州連

合整合化立法が適用され得るといことが基本原則である。この規則の要件に包摂されている AI システムの危険は、現行の欧州連合整合化立法とは異なる側面と関係しており、それゆえ、この規則の要件は、欧州連合整合化立法の現行の本体部分を補完することになるだろう。例えば、AI システムを組み込んでいる機械製品または医療機器製品は、その部門別立法が AI システムに特有のリスクを取扱っていないため、関連する欧州連合整合化立法に定める健康と安全の必須要件によって対処されていないリスクを示し得る。このことは、様々な立法行為の同時的かつ補完的な適用を要求する。一貫性を確保するため、そして、無用な行政上の重複と無用な負担を避けるため、当該製品に対してこの規則の要件及び新たな立法枠組みを基礎としかつこの規則の別紙の中に列挙される欧州連合整合化立法の要件が適用される 1 または複数の高リスク AI システムを含んでいる製品の提供者は、欧州連合整合化立法の全ての適用可能な要件を 1 または複数の高リスク AI システムを含んでいる製品の最適化された態様による遵守をどのように確保するかに関する業務運営上の判断に関し、柔軟性をもつべきである。その柔軟性は、例えば、新たな立法枠組みを基礎としかつこの規則の別紙の中に列挙される現行の欧州連合整合化立法の下において要求されている既存の文書または手続の中に、この規則の下において要求されている必要的な試験過程と報告過程、情報及び文書の一部を統合するための提供者による判断のことを意味し得る。このことは、いかなる方法によっても、適用可能な全ての要件を遵守すべき提供者の義務を損ねてはならない。

To mitigate the risks from high-risk AI systems placed on the market or put into service and to ensure a high level of trustworthiness, certain mandatory requirements should apply to high-risk AI systems, taking into account the intended purpose and the context of use of the AI system and according to the risk-management system to be established by the provider. The measures adopted by the providers to comply with the mandatory requirements of this Regulation should take into account the generally acknowledged state of the art on AI, be proportionate and effective to meet the objectives of this Regulation. Based on the New Legislative Framework, as clarified in Commission notice ‘The ‘Blue Guide’ on the implementation of EU product rules 2022’, the general rule is that more than one legal act of Union harmonisation legislation may be applicable to one product, since the making available or putting into service can take place only when the product complies with all applicable Union harmonisation legislation. The hazards of AI systems covered by the requirements of this Regulation concern different aspects than the existing Union harmonisation legislation and therefore the requirements of this Regulation would complement the existing body of the Union harmonisation legislation. For example, machinery or medical devices products incorporating an AI system might present risks not addressed by the essential health and safety requirements set out in the relevant Union harmonised legislation, as that sectoral law does not deal with risks specific to AI systems. This calls for a simultaneous and complementary application of the various legislative acts. To ensure consistency and to avoid an unnecessary administrative burden and unnecessary costs, providers of a product that contains one or more high-risk AI system, to which the requirements of this Regulation and of the Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all the applicable requirements of that Union harmonised legislation in an optimal manner. That flexibility could mean, for example a decision by the provider to integrate a part of the necessary testing and reporting processes, information and documentation required under this Regulation into already existing documentation and procedures required under existing Union harmonisation legislation based on the New Legislative

Framework and listed in an annex to this Regulation. This should not, in any way, undermine the obligation of the provider to comply with all the applicable requirements.

- (65) リスク管理システムは、高リスク AI システムの全ライフサイクルを通じて計画され及び実行される継続的で反復的なプロセスによって構成されるべきである。このプロセスは、健康、安全及び基本的な権利に対する AI システムの関連リスクを発見し及び緩和することを狙いとするべきである。リスク管理システムは、そのリスク管理システムの継続的な実効性を確保し、かつ、この規則に従ってとられた重要な判断及び行動の正当性及び文書化を確保するため、定期的に見直され及びアップデートされるべきである。このプロセスは、提供者がリスクまたは負の影響を発見することを確保し、かつ、当該 AI システムと同システムが運用される環境との間の相互作用から生ずる可能性のあるリスクを含め、そのシステムの所期の目的に照らし、健康、安全及び基本的な権利に対する AI システムの既知のリスク及び合理的に予測可能なリスク並びに合理的に予測可能な濫用に対する緩和の方策を実装することを確保すべきである。リスク管理システムは、AI における最新技術に照らし、最も適切なリスク管理の方策を採用すべきである。最も適切なリスク管理の方策を見出す際、提供者は、行われた選択を文書化し及び説明すべきであり、また、それが関連するときは、専門家及び外部の利害関係者を関与させるべきである。高リスク AI システムの合理的に予測可能な濫用を発見する際、提供者は、所期の目的には直接的には包摂されておらず、かつ、使用説明書の中では定められていないとしても、それでもなお、特定の AI システムの特性及び使用という文脈において、自明的に予測可能となっている人間の行動から帰結すると合理的に予測可能な AI システムの利用を包摂すべきである。所期の目的に従った、または、合理的に予測可能な濫用の諸条件の下における高リスク AI システムの利用と関連する既知または予測可能な状況であって、健康及び安全または基本的な権利に対するリスクを導き得る状況は、その提供者から提供される使用説明書の中に含まれるべきである。それは、高リスク AI システムを利用する際に設置者がそれに気づき、かつ、考慮に入れることを確保するためである。この規則の下において予測可能な濫用に対するリスク緩和の方策を見出すこと及び実装することは、予測可能な濫用に対処するための提供者によるその高リスク AI システムの特別の付加的な訓練を要求してはならない。ただし、提供者は、必要に応じて、かつ、しかるべく、合理的に予測可能な濫用を緩和するためのそのような付加的な訓練の方策を検討することが推奨される。

The risk-management system should consist of a continuous, iterative process that is planned and run throughout the entire lifecycle of a high-risk AI system. That process should be aimed at identifying and mitigating the relevant risks of AI systems on health, safety and fundamental rights. The risk-management system should be regularly reviewed and updated to ensure its continuing effectiveness, as well as justification and documentation of any significant decisions and actions taken subject to this Regulation. This process should ensure that the provider identifies risks or adverse impacts and implements mitigation measures for the known and reasonably foreseeable risks of AI systems to the health, safety and fundamental rights in light of their intended purpose and reasonably foreseeable misuse, including the possible risks arising from the interaction between the AI system and the environment within which it operates. The risk-management system should adopt the most appropriate risk-management measures in light of the state of the art in AI. When identifying the most appropriate risk-management measures, the provider should document and explain the choices made and, when relevant, involve experts and external stakeholders. In identifying the reasonably foreseeable misuse of high-risk AI systems, the provider should cover uses of AI systems which, while not directly covered by the intended

purpose and provided for in the instruction for use may nevertheless be reasonably expected to result from readily predictable human behaviour in the context of the specific characteristics and use of a particular AI system. Any known or foreseeable circumstances related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights should be included in the instructions for use that are provided by the provider. This is to ensure that the deployer is aware and takes them into account when using the high-risk AI system. Identifying and implementing risk mitigation measures for foreseeable misuse under this Regulation should not require specific additional training for the high-risk AI system by the provider to address foreseeable misuse. The providers however are encouraged to consider such additional training measures to mitigate **reasonable** foreseeable misuses as necessary and appropriate.

- (66) 要件は、リスク管理、使用されるデータセットの品質及び適合性、技術文書及び記録の保管、透明性及び設置者に対する情報の提供、人間による監視、並びに、堅牢性、正確性及びサイバーセキュリティに関し、高リスク AI システムに対して適用されるべきである。それらの要件は、健康、安全及び基本的な権利に対するリスクを実効的に緩和するために必要である。合理的に利用可能なより取引制限的な措置が存在しないので、それらの要件は、取引に対する正当化されない制限ではない。

Requirements should apply to high-risk AI systems as regards risk management, the quality and relevance of data sets used, technical documentation and record-keeping, transparency and the provision of information to deployers, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights. As no other less trade restrictive measures are reasonably available those requirements are not unjustified restrictions to trade.

- (67) 高リスク AI システムが意図されたとおりにかつ安全に性能を発揮し、欧州連合法によって禁止されている差別の発生源とならないことを確保するという観点から、特にモデルの訓練を含む技法が用いられる場合、高品質のデータ及び高品質のデータへのアクセスは、多くの AI システムの構造を提供すること及びその性能を確保することにおいて、重要な役割を演じている。訓練、検証及び試験の高品質のデータセットは、適切なデータ統治及び運営管理実務の実装を要求する。そのラベルを含め、訓練、検証及び試験のためのデータセットは、そのシステムの所期の目的の観点から、適合性があり、十分な代表比率があり、かつ、可能な最善の範囲内でエラーがなくかつ完全であるべきである。規則(EU) 2016/679 のような欧州連合のデータ保護法の遵守を容易にするため、個人データの場合においては、データ統治及び運営管理実務は、データ収集の当初の目的に関する透明性を含めるべきである。当該の個人または個人のグループとの関係において高リスク AI システムが利用されることが意図されている個人または個人のグループとの関連するものを含め、個人の健康及び安全に影響を与え、基本的な権利に負の影響を与え、または、欧州連合法の下において禁止されている差別を導くおそれのあるデータセット内のあり得るバイアスの緩和に特別の注意を払い、特に、データ出力が将来の運用のための入力に対して影響を与える場合(「フィードバックループ」)において、データセットは、適切な統計特性ももつべきである。例えば、特に、過去のデータが使用されている場合、または、そのシステムが実世界の設定の中で実装されているときに生成される場合、バイアスは、基盤となるデータセットに固有のものであり得る。AI システムから提供される結果は、とりわけ、人種または民族のグループを含め一定の脆弱性のあるグループに属する人々にとって、既存の差別を

徐々に増加させる傾向があり、それによって既存の差別を永続化及び拡大させるような固有のバイアスによって影響を受けることがあり得る。データセットが可能な最善の範囲内で完全でありかつエラーのないものであるべきであるとの要件は、AI システムの開発及び試験の過程におけるプライバシー保護技法の利用に対して影響を与えてはならない。とりわけ、データセットは、当該システムの所期の目的によって要求される範囲内において、当該 AI システムが利用されることが意図されている個々の地理的な、文脈上の、行動上のまたは機能上の設定に特有の機能、特性または要素を考慮に入れるべきである。データ統治と関連する要件は、この規則のデータ要件の遵守が確保されている限り、データ統治の検証、データセットの完全性及びデータの訓練、検証及び試験の実務を含め、認証された遵守のサービスを提供する第三者に対して依頼することによって遵守され得る。

High-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems, especially when techniques involving the **training of models** are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become a source of discrimination prohibited by Union law. High-quality **data sets** for training, validation and testing require the implementation of appropriate data governance and management practices. **Data sets** for training, validation and testing, including the labels, should be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose of the system. In order to facilitate compliance with Union data protection law, such as Regulation (EU) 2016/679, data governance and management practices should include, in the case of personal data, transparency about the original purpose of the data collection. The data sets should also have the appropriate statistical properties, including as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used, with specific attention to the mitigation of possible biases in the data sets, that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations (feedback loops). Biases can for example be inherent in underlying data sets, especially when historical data is being used, or generated when the systems are implemented in real world settings. Results provided by AI systems could be influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable groups, including racial or ethnic groups. The requirement for the data sets to be to the best extent possible **complete and free of errors** should not affect the use of privacy-preserving techniques in the context of the development and testing of AI systems. In particular, data sets should take into account, to the extent required by their intended purpose, the features, characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting **which** the AI system is intended to be used. The requirements related to data governance can be complied with by having recourse to third parties that offer certified compliance services including verification of data governance, **data set** integrity, and data training, validation and testing practices, as far as compliance with the data requirements of this Regulation are ensured.

- (68) 高リスク AI システムの開発及び評価に関して、提供者、指定組織のような一定の関与者、並びに、それら以外の、欧州デジタル技術革新ハブ、試験実験施設及び調査研究者のような適格な法主体は、この規則と関連をもつ関与者それぞれの活動分野内にある高品質のデータセットにアクセスし及びそれを利用できるべきである。欧州委員会によって設けられる欧州共通データ空間、並びに、企業と政府との間の公共の利益におけるデータ共有の促進は、AI システムの訓練、検証及び試験の

ための高品質データへの信頼でき、説明責任のある、かつ、非差別のアクセスを提供するための道具となる。例えば、医療において、欧州医療データ空間は、プライバシーを保護し、安全であり、適時であり、透明性がありかつ信頼できる態様により、かつ、適切な組織的統治により、医療データへの非差別のアクセスを促進し、また、そのデータセットに対する AI アルゴリズムの訓練を促進することになる。部門別の機関を含め、データへのアクセスを提供または支援する適格な職務権限のある関連機関もまた、AI システムの訓練、検証及び試験のための高品質データの提供を支援し得る。

For the development and assessment of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as European Digital Innovation Hubs, testing experimentation facilities and researchers, should be able to access and use high-quality data sets within the fields of activities of those actors which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high-quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of AI algorithms on those data sets, in a privacy-preserving, secure, timely, transparent and trustworthy manner; and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

- (69) プライバシー及び個人データの保護の権利は、AI システムの全ライフサイクルを通して保障されなければならない。この点に関し、欧州連合のデータ保護法に定めるようなデータのミニマム化の原則並びにバイデザイン及びバイデフォルトのデータ保護の原則は、個人データが処理される際に適用可能である。この規則に定めるデータ統治に関する要件を妨げることなく、それらの原則の遵守を確保するために提供者によってとられる方策は、匿名化と暗号化だけでなく、データにアルゴリズムを組み込めるようにする技術の利用も含め得るのであり、また、関係者間におけるやりとりまたは生のデータもしくは構造化されたデータそれ自体を複製することなく AI システムを訓練することを許容する。

The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed. Measures taken by providers to ensure compliance with those principles may include not only anonymisation and encryption, but also the use of technology that permits algorithms to be brought to the data and allows training of AI systems without the transmission between parties or copying of the raw or structured data themselves, without prejudice to the requirements on data governance provided for in this Regulation.

- (70) AI システム内のバイアスから帰結し得る差別に対して他者の権利を保護するため、その提供者は、例外として、高リスク AI システムと関係するバイアスの検出及び修正を確保する目的のために厳格に必要な範囲内で、自然人の基本的な権利及び自由のための適切な安全確保に服し、かつ、規則(EU) 2016/679、規則(EU) 2018/1725 及び指令(EU) 2016/680 に定める条件に加え、この規則の下において定められる全ての適用可能な条件を適用した上で、規則(EU) 2016/679 の第 9 条第 2 項(g)及び

規則(EU) 2018/1725 の第 10 条第 2 項(g)の意味における重大な公共の利益の事実として、特別類型の個人データも処理できるべきである。

In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should, exceptionally, to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons and following the application of all applicable conditions laid down under this Regulation in addition to the conditions laid down in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, be able to process also special categories of personal data, as a matter of substantial public interest within the meaning of Article 9(2), point (g) of Regulation (EU) 2016/679 and Article 10(2), point (g) of Regulation (EU) 2018/1725.

- (71) 高リスク AI システムがどのようにして開発されたのか、及び、当該システムのライフタイムを通して当該システムがどのように性能を発揮するのかに関する理解しやすい情報をもつことは、当該システムの追跡可能性を実現可能にするため、この規則の下にある要件の遵守を検証するため、並びに、当該システムの運用及び市場化後監視のために必須である。このことは、当該 AI システムの関連要件の遵守を評価するため及び市場化後監視を容易にするために必要となる情報を含んでいる記録の保存及び技術文書の可用性を要求する。そのような情報は、そのシステムの一般的な特徴、実現能力及び制限、使用されたアルゴリズム、データ、訓練、試験及び検査のプロセス、並びに、適格なリスク管理システムに関する文書を含むべきであり、明確かつ理解しやすい方式で描述されるべきである。技術文書は、当該 AI システムのライフタイムを通して適切に、最新の状態に維持されるべきである。更に、高リスク AI システムは、当該システムのライフタイムの全期間にわたり、ログという手段によって、イベントの自動的な記録が技術的に可能であるべきである。

Having comprehensible information on how high-risk AI systems have been developed and how they perform throughout their lifetime is essential to enable traceability of those systems, verify compliance with the requirements under this Regulation, as well as monitoring of their operations and **post market monitoring**. This requires keeping records and the availability of technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements and facilitate **post market monitoring**. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk-management system and **drawn** in a clear and comprehensive form. The technical documentation should be kept up to date, appropriately throughout the lifetime of the AI system. Furthermore, high-risk AI systems should technically allow for the automatic recording of events, by means of logs, over the duration of the lifetime of the system.

- (72) 一定の AI システムの不透明性及び複雑性に関する懸念に対処するため、及び、この規則の下にある設置者の義務が設置者が満たすことを助けるため、当該システムが市場に置かれたりまたはサービスに供される前に、高リスク AI システムに対して透明性が要求されるべきである。高リスク AI システムは、設置者が、当該 AI システムがどのように動作するかを理解でき、そのシステムの機能性を評価でき、かつ、そのシステムの強度及び制限を了解できるようにする態様で設計されるべきである。高リスク AI システムは、使用説明書という方式により、適切な情報が添付されるべきである。そのような情

報は、当該 AI システムの性能の性質、実現能力及び制限を含めるべきである。その情報は、設置者によるその AI システムの出力の解釈を容易にするための手段を含め、提供者によって事前に決定されかつ適合性評価された変更に関する、及び、関連する人間による監視手段に関するシステムのふるまい及び稼働に影響を及ぼすかもしれない設置者の行動であって、その行動の下において健康、安全及び基本的な権利に対するリスクをその AI システムが導き得るものを含め、当該高リスク AI システムの利用と関連する既知であり得る状況及び予測可能であり得る状況に関する情報を包摂し得る。使用説明書を添付することを含め、透明性は、当該システムの利用において設置者を補助すべきであり、また、設置者によって行われる説明を受けた上での判断を支援すべきである。就中、設置者は、当該設置者に対して適用可能な義務に照らし、その設置者が利用を意図しているシステムを正しく選択するためのより良い立場にあるべきであり、意図された利用及び除外された利用に関して教育を受けるべきであり、かつ、当該 AI システムを正確かつ適切に利用すべきである。使用説明書の中に含まれている情報の読みやすさとアクセシビリティを拡大するため、それが適切なときは、例えば、制限に関するイラストによる例示並びに当該 AI システムの意図された利用及び除外された利用に関するイラストによる例示が含まれるべきである。提供者は、対象とする設置者の需要及び想定可能な知識を考慮に入れた上で、使用説明書を含め全ての文書が、意味のある、分かりやすく、アクセス可能かつ理解可能な情報を含むことを確保すべきである。使用説明書は、関係する構成国によって定められるとおり、対象とする設置者によって容易に理解され得る言語によって利用できるようにされるべきである。

To address concerns related to opacity and complexity of certain AI systems and help deployers to fulfil their obligations under this Regulation, transparency should be required for high-risk AI systems before they are placed on the market or put it into service. High-risk AI systems should be designed in a manner to enable deployers to understand how the AI system works, evaluate its functionality, and comprehend its strengths and limitations. High-risk AI systems should be accompanied by appropriate information in the form of instructions of use. Such information should include the characteristics, capabilities and limitations of performance of the AI system. Those would cover information on possible known and foreseeable circumstances related to the use of the high-risk AI system, including deployer action that may influence system behaviour and performance, under which the AI system can lead to risks to health, safety, and fundamental rights, on the changes that have been pre-determined and assessed for conformity by the provider and on the relevant human oversight measures, including the measures to facilitate the interpretation of the outputs of the AI system by the deployers. Transparency, including the accompanying instructions for use, should assist deployers in the use of the system and support informed decision making by them. Deployers should, inter alia, be in a better position to make the correct choice of the system that they intend to use in light of the obligations applicable to them, be educated about the intended and precluded uses, and use the AI system correctly and as appropriate. In order to enhance legibility and accessibility of the information included in the instructions of use, where appropriate, illustrative examples, for instance on the limitations and on the intended and precluded uses of the AI system, should be included. Providers should ensure that all documentation, including the instructions for use, contains meaningful, comprehensive, accessible and understandable information, taking into account the needs and foreseeable knowledge of the target deployers. Instructions for use should be made available in a language which can be easily understood by target deployers, as determined by the Member State concerned.

- (73) 高リスク AI システムは、自然人がその稼働を監視でき、そのシステムが意図されたように利用されることを確保し、かつ、そのシステムのライフサイクル全部にわたり、それらの影響が対処されるような方法で設計及び開発されるべきである。その目的のために、当該システムが市場に置かれまたはサービスに供される前に、そのシステムの提供者によって、人間による適切な監視手段が識別されるべきである。とりわけ、それが適切なときは、そのような手段は、当該システムそれ自体によっては優先され得ずかつ人間の運用者に対して応答する内部に組み込まれた業務運営上の制約にそのシステムが服すること、そして、人間による監視の任務を与えられた自然人がその役割を遂行するための必要な能力、訓練及び権限をもつことを保証すべきである。負の結果もしくはリスクを避けるために介入するかどうか、いつ、どのように介入するかの説明を受けた上での判断を行うため、または、当該システムが意図された性能を発揮しない場合にはそのシステムを停止させるため、人間による監視の任務を与えられた自然人に対して指針と情報を提供するための仕組みを当該高リスク AI システムが内包することをしかるべく確保することも必須である。一定の生体要素識別システムによる不正確なマッチの場合における個人に対する重大な結果を考慮し、同システムに関する拡大された人間による監視の要件を定め、少なくとも 2 名の自然人によってそれが隔離して検証及び確認されたのではない限り、そのシステムから帰結する識別を基礎とするいかなる行動または判断も設置者によって行われ得ないようにすることが適切である。その自然人は、1 または複数の法主体からの者であることができ、そのシステムを運用または利用する者を含め得る。この要件は、無用の負担または遅延を呈するものであってはならず、かつ、異なる者による隔離検証は当該システムによって生成されるログの中に自動的に記録されることで十分であり得る。法執行、移民、出入国管理及び難民の分野の特殊性に鑑み、この要件は、同要件を適用することが不適切であると欧州連合法または国内法が判断するとき、適用してはならない。

High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning, ensure that they are used as intended and that **their impacts** are addressed over the system's lifecycle. To that end, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role. It is also essential, as appropriate, to ensure that high-risk AI systems include mechanisms to guide and inform a natural person to whom human oversight has been assigned to make informed decisions if, when and how to intervene in order to avoid negative consequences or risks, or stop the system if it does not perform as intended. Considering the significant consequences for persons in the case of an incorrect match by certain biometric identification systems, it is appropriate to provide for an enhanced human oversight requirement for those systems so that no action or decision may be taken by the deployer on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons. Those persons could be from one or more entities and include the person operating or using the system. This requirement should not pose unnecessary burden or delays and it could be sufficient that the separate verifications by the different persons are automatically recorded in the logs generated by the system. Given the specificities of the areas of law enforcement, migration, border control and asylum, this requirement should not apply where Union or national law **considers** the application of that requirement to be disproportionate.

- (74) 高リスク AI システムは、そのシステムのライフサイクルを通して一貫性をもって性能を発揮すべきであり、また、所期の目的に照らし、かつ、一般に承認された最新技術に従い、適切なレベルの正確性、堅牢性及びサイバーセキュリティに適合すべきである。欧州委員会並びに適格な組織及び利害関係者は、AI システムのリスク及び負の影響の緩和を適正に考慮することが推奨される。添付される使用説明書の中で、期待されるレベルの性能測定基準が宣言されるべきである。提供者は、設置者に対し、明確かつ容易に理解できる方法で、誤読または誤導の文言なく、この情報を伝達することが求められる。欧州議会及び理事会の指令 2014/31/EU³⁵及び指令 2014/32/EU³⁶を含め、適法な計量に関する欧州連合法は、計量の正確性を確保すること並びに商取引の透明性及び公正性を助けることを狙いとしている。この文脈において、欧州委員会は、計量当局及びベンチマーキング当局のような適格な利害関係者及び組織と協力して、AI システムのためのベンチマーク及び測定手法の開発をしかるべく推進すべきである。そのようにする際、欧州委員会は、AI システムと関連する計量及び適格な測定指標に関して作業している国際的なパートナーの動向に注意し、かつ、それと共働すべきである。

High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity, in light of their intended purpose and in accordance with the generally acknowledged state of the art. The Commission and relevant organisations and stakeholders are encouraged to take due consideration of the mitigation of risks and the negative impacts of the AI system. The expected level of performance metrics should be declared in the accompanying instructions of use. Providers are urged to communicate that information to deployers in a clear and easily understandable way, free of misunderstandings or misleading statements. Union law on legal metrology, including Directives 2014/31/EU⁽³⁵⁾ and 2014/32/EU⁽³⁶⁾ of the European Parliament and of the Council, aims to ensure the accuracy of measurements and to help the transparency and fairness of commercial transactions. In that context, in cooperation with relevant stakeholders and organisation, such as metrology and benchmarking authorities, the Commission should encourage, as appropriate, the development of benchmarks and measurement methodologies for AI systems. In doing so, the Commission should take note and collaborate with international partners working on metrology and relevant measurement indicators relating to AI.

- (75) 技術上の堅牢性は、高リスク AI システムにとって鍵となる要件の 1 つである。高リスク AI システムは、システム内の制限から生じ得る、または、そのシステムを運用する環境から生じ得る危険なふるまいまたはそれ以外の望ましくないふるまい(例: エラー、障害、一貫性の欠如、想定外の状況)との関係において、回復力をもつべきである。それゆえ、例えば、危険なふるまいまたはそれ以外の望ましくないふるまいを防止またはミニマム化するための適切な技術上のソリューションを設計すること及び

³⁵ 非自動計量器市場で利用できるようにすることと関連する構成国の法律の整合化に関する欧州議会及び理事会の 2014 年 2 月 26 日の指令 2014/31/EU (OJ L 96, 29.3.2014, p. 107).

Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments (OJ L 96, 29.3.2014, p. 107).

³⁶ 計量器市場で利用できるようにすることと関連する構成国の法律の整合化に関する欧州議会及び理事会の 2014 年 2 月 26 日の指令 2014/32/EU (OJ L 96, 29.3.2014, p. 149).

Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (OJ L 96, 29.3.2014, p. 149).

開発することによって、高リスク AI システムの堅牢性を確保するための技術上及び組織上の方策がとられるべきである。それらの技術上のソリューションは、例えば、一定の異常が現れる際、または、事前に定められた一定の限界から外れて運用が行われる場合において、そのシステムがその運用を安全に中断できるようにする仕組み(フェイルセーフ計画)を含め得る。それらのリスクに対する防護に失敗することは、例えば、AI システムによって生成される誤りのある判定または悪い出力もしくはバイアスのかかった出力によって、基本的な権利に対する安全上の影響または負の影響を導き得る。

Technical robustness is a key requirement for high-risk AI systems. They should be resilient in relation to harmful or otherwise undesirable behaviour that may result from limitations within the systems or the environment in which the systems operate (e.g. errors, faults, inconsistencies, unexpected situations). Therefore, technical and organisational measures should be taken to ensure robustness of high-risk AI systems, for example by designing and developing appropriate technical solutions to prevent or minimise harmful or otherwise undesirable behaviour. Those technical solution may include for instance mechanisms enabling the system to safely interrupt its operation (fail-safe plans) in the presence of certain anomalies or when operation takes place outside certain predetermined boundaries. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system.

- (76) サイバーセキュリティは、システムの脆弱性を悪用する悪意ある第三者による、AI システムの利用、ふるまい、性能を改変し、または、そのシステムのセキュリティ上の特性を混乱させようとする試みに抗して AI システムが回復力をもつことを確保する上で重要な役割を演じている。AI システムを対象とするサイバー攻撃は、訓練データセット(例: データ汚染攻撃)もしくは訓練されたモデル(例: 敵対的訓練攻撃もしくはメンバーシップ推論攻撃)のような AI に固有の資産を利用し、または、AI システムのデジタル資産もしくはその基盤となる ICT インフラの脆弱性を悪用し得る。それゆえ、そのリスクに対して適切なサイバーセキュリティのレベルを確保するため、基盤となる ICT インフラもしかるべく考慮に入れた上で、高リスク AI システムの提供者によって、セキュリティ上の管理策のような適切な方策がとられるべきである。

Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as **training data sets** (e.g. data poisoning) or trained models (e.g. adversarial attacks or membership inference), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures, such as security controls, should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.

- (77) この規則に定める堅牢性及び正確性と関連する要件を妨げることなく、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則の適用範囲内にある高リスク AI システムは、同規則に従い、同規則に定めるサイバーセキュリティ上の必須の要件を満たすことにより、この規則のサイバーセキュリティ上の要件の遵守を示し得る。高リスク AI システムが、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の

規則の必須の要件を満たすときは、そのシステムは、同規則の下において発行される EU 適合性宣言書またはその一部の中で当該要件が達成されていることが示されている限り、この規則に定めるサイバーセキュリティ上の要件を遵守していると推定されるべきである。その目的のために、この規則に従って高リスク AI システムとして分類されたデジタルの要素をもつ製品と関連し、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則の下において実行されるサイバーセキュリティ上のリスクの評価は、データ汚染攻撃または敵対的訓練攻撃のような AI に固有の脆弱性を含め、当該 AI システムの利用、ふるまいまたは性能を改変するための無権限の第三者による試みと関連する AI システムのサイバー回復力に対するリスクを顧慮すべきであり、また、それが適格であるときは、この規則によって要求される基本的な権利に対するリスクを考慮すべきである。

Without prejudice to the requirements related to robustness and accuracy set out in this Regulation, high-risk AI systems which fall within the scope of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, in accordance with that regulation may demonstrate compliance with the cybersecurity requirements of this Regulation by fulfilling the essential cybersecurity requirements set out in that regulation. When high-risk AI systems fulfil the essential requirements of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, they should be deemed compliant with the cybersecurity requirements set out in this Regulation in so far as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

- (78) この規則によって提供される適合性評価手続は、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則によって包摂され、かつ、この規則の下において高リスク AI システムとして分類されたデジタルの要素をもつ製品のサイバーセキュリティ上の必須の要件との関係において適用されるべきである。ただし、この原則は、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則の適用のあるデジタルの要素をもつ不可欠の製品にとって必要となる保証のレベルを緩和してはならない。それゆえ、この原則からの特例により、この規則の適用範囲内にあり、かつ、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則によりデジタルの要素をもつ重要製品及び不可欠製品としても分類される高リスク AI システムであって、この規則の別紙の中で定められる内部統制を基礎とする適合性評価手続が適用されるものは、デジタルの要素をもつ製品のサイバーセキュリティの横断的な要件に関する欧州議会及び理事会の規則のサイバーセキュリティ上の必須の要件が関係する限り、同規則の適合性評価の諸条項に服する。この場合、この規則に包摂されるサイバーセキュリティ以外の全ての側面に関し、この規則の別紙の中で定められる内部統制を基礎とする適合性評価に関する諸条項がそれぞれ適用されるべきである。サイバーセキュリ

ティ上の基本方針に関する ENISA の知識と経験並びに欧州議会及び理事会の規則(EU) 2019/881³⁷ の下において ENISA に対して割当てられた職務を基礎として、欧州委員会は、AI システムのサイバーセキュリティと関連する検討課題に関し、ENISA と協力すべきである。

The conformity assessment procedure provided by this Regulation should apply in relation to the essential cybersecurity requirements of a product with digital elements covered by a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and classified as a high-risk AI system under this Regulation. However, this rule should not result in reducing the necessary level of assurance for critical products with digital elements covered by a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. Therefore, by way of derogation from this rule, high-risk AI systems that fall within the scope of this Regulation and are also qualified as important and critical products with digital elements pursuant to a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and to which the conformity assessment procedure based on internal control set out in an annex to this Regulation applies, are subject to the conformity assessment provisions of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements insofar as the essential cybersecurity requirements of that regulation are concerned. In this case, for all the other aspects covered by this Regulation the respective provisions on conformity assessment based on internal control set out in an annex to this Regulation should apply. Building on the knowledge and expertise of ENISA on the cybersecurity policy and tasks assigned to ENISA under the Regulation (EU) 2019/881 of the European Parliament and of the Council⁽³⁷⁾, the Commission should cooperate with ENISA on issues related to cybersecurity of AI systems.

- (79) 当該自然人または法人が当該システムを設計または開発した者であるか否かに拘らず、高リスク AI システムを市場に置くことまたはサービスに供することに関し、提供者として定義される特定の自然人または法人が責任を負うことが適切である。

It is appropriate that a specific natural or legal person, defined as the provider, takes responsibility for the placing on the market or the putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.

- (80) 障害のある者の権利に関する国連条約への署名により、欧州連合及び構成国は、障害をもつ人々を差別から保護すること、障害をもつ者の平等を促進すること、障害をもつ者が、他者との間において平等ベースで、情報通信の技術とシステムへのアクセスをもつことを確保すること、そして、障害をもつ者に関するプライバシーの尊重を確保することが法的に義務づけられる。AI システムの重要性

³⁷ ENISA (欧州連合サイバーセキュリティ局) に関する、及び、情報通信技術のサイバーセキュリティ認証に関する、並びに、規則(EU) No 526/2013 を廃止する欧州議会及び理事会の 2019 年 4 月 17 日の規則(EU) 2019/881 (サイバーセキュリティ法) (OJ L 151, 7.6.2019, p. 15).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

とその利用の増加に鑑み、全ての新技术及び新サービスに対するユニバーサルデザインの原則の適用は、それらの者の生来の尊厳及び多様性を全面的に考慮に入れた方法により、障害をもつ人々を含め、AI技術によって潜在的に影響を受ける全ての者またはAI技術を利用する全ての者に対する全面的かつ平等なアクセスを確保すべきである。それゆえ、欧州議会及び理事会の指令(EU) 2016/2102³⁸並びに指令(EU) 2019/882を含め、アクセシビリティの要件を提供者が全面的に遵守することを確保することが必須である。提供者は、それらの要件をバイデザインで遵守することを確保すべきである。それゆえ、必要な方策は、可能な限り全部、高リスク AI システムの設計の中に統合されるべきである。

As signatories to the United Nations Convention on the Rights of Persons with Disabilities, the Union and the Member States are legally obliged to protect persons with disabilities from discrimination and promote their equality, to ensure that persons with disabilities have access, on an equal basis with others, to information and communications technologies and systems, and to ensure respect for privacy for persons with disabilities. Given the growing importance and use of AI systems, the application of universal design principles to all new technologies and services should ensure full and equal access for everyone potentially affected by or using AI technologies, including persons with disabilities, in a way that takes full account of their inherent dignity and diversity. It is therefore essential that providers ensure full compliance with accessibility requirements, including Directive (EU) 2016/2102 of the European Parliament and of the Council⁽³⁸⁾ and Directive (EU) 2019/882. Providers should ensure compliance with these requirements by design. Therefore, the necessary measures should be integrated as much as possible into the design of the high-risk AI system.

- (81) 提供者は、良好な品質管理システムを設け、要求される適合性評価手続を完了することを確保し、関連文書を作成し、そして、堅牢な市場化後監視システムを設けるべきである。欧州連合の関連する部門別の法律の下にある品質管理システムと関連する義務に服する高リスク AI システムの提供者は、欧州連合の他の部門別の法律に定める既存の品質管理システムの一部として、この規則に定める品質管理システムの要素を含める可能性をもつべきである。この規則と既存の部門別の欧州連合法との間の補完性は、将来の標準化活動または欧州委員会によって採択される指針の中においても考慮に入れられるべきである。当該行政機関自身の利用のために高リスク AI システムをサービスに供する行政機関は、しかるべく、当該部門の特性並びに当の行政機関の職務権限及び組織構成を考慮に入れた上で、国内レベルまたは地域レベルで採択された品質管理システムの一部として、品質管理システムに関する規定を採択及び実装できる。

The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. Providers of high-risk AI systems that are subject to obligations regarding quality management systems under relevant sectoral Union law should have the possibility to include the elements of the quality management system

³⁸ 公的部門の組織の Web サイト及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欧州議会及び理事会の 2016 年 10 月 26 日の指令(EU)2016/2102(OJ L327, 2.12.2016, p. 1).

Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies(OJ L327, 2.12.2016, p. 1).

provided for in this Regulation as part of the existing quality management system provided for in that other sectoral Union law. The complementarity between this Regulation and existing sectoral Union law should also be taken into account in future standardisation activities or guidance adopted by the Commission. Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority concerned.

- (82) この規則を執行できるようにするため、及び、運用者のための平等な競争の場を創設するため、そして、デジタル製品を利用できるようにする異なる形態を考慮に入れた上で、全ての状況の下において、欧州連合内に拠点をもつ者が、当局に対し、AIシステムの遵守に関する必要な全ての情報を提供できることを確保することが重要である。それゆえ、欧州連合内において当該の者の AI システムが利用できるようにされる前に、第三国内に拠点をもつ提供者は、書面による委任により、欧州連合内に拠点をもつ権限のある代理人に委任すべきである。この権限のある代理人は、欧州連合内に拠点をもたず、当該提供者によって欧州連合内において市場に置かれまたはサービスに供された高リスク AI システムの法令遵守を確保する上で、そして、その提供者の欧州連合内に拠点をもつ連絡担当者としての役務を提供する上で、極めて重要な役割を演ずる。

To enable enforcement of this Regulation and create a level playing field for operators, and, taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary information on the compliance of an AI system. Therefore, prior to making their AI systems available in the Union, providers established in third countries should, by written mandate, appoint an authorised representative established in the Union. This authorised representative plays a pivotal role in ensuring the compliance of the high-risk AI systems placed on the market or put into service in the Union by those providers who are not established in the Union and in serving as their contact person established in the Union.

- (83) AI システムのための価値連鎖の性質及び複雑性に照らし、かつ、新たな立法枠組みに沿って、法的確実性を確保すること及びこの規則の遵守を容易にすることが必須である。それゆえ、AI システムの開発に寄与し得る輸入業者及び流通業者のような、当該価値連鎖の流れの中にある適格な運用者の役割及び個別の義務を明確にする必要がある。一定の状況下においては、それらの運用者は、同時に複数の役割をもって行動することがあり得るのであり、それゆえ、それらの役割と関係する全ての関連義務を累積的に満たすべきである。例えば、ある運用者は、同時に、流通業者及び輸入業者として行動し得る。

In light of the nature and complexity of the value chain for AI systems and in line with the New Legislative Framework, it is essential to ensure legal certainty and facilitate the compliance with this Regulation. Therefore, it is necessary to clarify the role and the specific obligations of relevant operators along that value chain, such as importers and distributors who may contribute to the development of AI systems. In certain situations those operators could act in more than one role at the same time and should therefore fulfil cumulatively all relevant obligations associated with those roles. For example, an operator could act as a distributor and an importer at the same time.

- (84) 法的確実性を確保するため、一定の個別の条件の下において、流通業者、輸入業者、設置者またはそれ以外の第三者が高リスク AI システムの提供者であると判断されるべきであり、そして、それゆえ、関連する全ての義務を負うことを明確にする必要がある。義務が別異に割当てられることを定める契約による合意事項を妨げることなく、既に市場に置かれもしくはサービスに供された高リスク AI システム上に、当該関係者がその名称もしくは商標を付す場合は、その場合であり得る。この規則に従って高リスク AI システムであることを維持したままで既に市場に置かれもしくは既にサービスに供されている高リスク AI システムに対して当該関係者が実質的な修正を行う場合、または、一般目的 AI システムを含め、高リスクとして分類されておらず、かつ、この規則に従って AI システムが高リスク AI システムになるような方法で既に市場に置かれもしくはサービスに供された AI システムの所期の目的を当該関係者が修正する場合もそのような場合であり得る。それらの条項は、新たな立法枠組みを基礎とする欧州連合の一定の整合化立法の中に定められており、この規則と共に適用されるべき、より細目的な条項を妨げることなく適用されるべきである。例えば、一定の修正が、適用可能な要件を当該機器が遵守することに影響を与え得る機器の改変であると判断してはならないことを定める規則(EU) 2017/745 の第 16 条第 2 項は、同規則の意味における医療機器である高リスク AI システムに対して適用され続けるべきである。

To ensure legal certainty, it is necessary to clarify that, under certain specific conditions, any distributor, importer, deployer or other third-party should be considered to be a provider of a high-risk AI system and therefore assume all the relevant obligations. This would be the case if that party puts its name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual **arrangements** stipulating that the obligations are allocated otherwise. This would also be the case if that party makes a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in a way that it remains a high-risk AI system in accordance with this Regulation, or if it modifies the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service, in a way that the AI system becomes a high-risk AI system in accordance with this Regulation. Those provisions should apply without prejudice to more specific provisions established in certain Union harmonisation legislation based on the New Legislative Framework, together with which this Regulation should apply. For example, Article 16(2) of Regulation (EU) 2017/745, establishing that certain changes should not be considered to be modifications of a device that could affect its compliance with the applicable requirements, should continue to apply to high-risk AI systems that are medical devices within the meaning of that Regulation.

- (85) 一般目的 AI システムは、それ自体として高リスク AI システムとして利用され得るのであり、または、別の高リスク AI システムのコンポーネントであり得る。それゆえ、一般目的 AI システムの特性のゆえに、かつ、AI 価値連鎖の流れに沿った責任の公正な分担を確保するため、そのようなシステムの提供者は、他の提供者によって一般目的 AI システムがそれ自体として高リスク AI システムとして利用され得るかまたは高リスク AI システムのコンポーネントとして利用され得るかを問わず、かつ、この規則の下において別異に定められていない限り、この規則の下にある関連義務をそれらの提供者が遵守できるようにするために適格な高リスク AI システムの提供者との間において、また、この規則の下において設置される職務権限のある機関との間において、緊密に協力すべきである。

General-purpose AI systems may be used as high-risk AI systems by themselves or be components of other high-risk AI systems. Therefore, due to their particular nature and in order to ensure a fair sharing of responsibilities along the AI value chain, the providers of such systems should, irrespective of whether they may be used as high-risk AI systems as such by other providers or as components of high-risk AI systems and unless provided otherwise under this Regulation, closely cooperate with the providers of the relevant high-risk AI systems to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation.

- (86) この規則の中で定められた条件下において、当該 AI システムを最初に市場に置きたりサービスに供した提供者が、この規則の目的のための提供者であると判断されなくなるべき場合であり、かつ、当該提供者が、当該 AI システムの高リスク AI システムへの変更を明示で排除しなかった場合、その元提供者は、それでもなお、とりわけ高リスク AI システムの適合性評価の遵守に関し、緊密に協力し、かつ、必要な情報を利用できるようにすべきであり、かつ、この規則に定める義務の履行のために要求され、合理的に期待される技術上のアクセス及びそれ以外の補助を提供すべきである。

Where, under the conditions laid down in this Regulation, the provider that initially placed the AI system on the market or put it into service should no longer be considered to be the provider for the purposes of this Regulation, and when that provider has not expressly excluded the change of the AI system into a high-risk AI system, the former provider should nonetheless closely cooperate and make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems.

- (87) 加えて、製品の安全性コンポーネントである高リスク AI システムであって、新たな立法枠組みを基礎とする欧州連合整合化立法の適用範囲内にあるものが、当該製品から独立して市場に置かれておらずまたはサービスに供されていないときは、同立法の中で定義された製品製造者は、この規則の中で設けられた提供者の義務を遵守すべきであり、かつ、とりわけ、最終製品の中に組み込まれた AI システムがこの規則の要件を遵守することを確保すべきである。

In addition, where a high-risk AI system that is a safety component of a product which falls within the scope of Union harmonisation legislation based on the New Legislative Framework is not placed on the market or put into service independently from the product, the product manufacturer defined in that legislation should comply with the obligations of the provider established in this Regulation and should, in particular, ensure that the AI system embedded in the final product complies with the requirements of this Regulation.

- (88) AI 価値連鎖の流れに沿って、しばしば、複数の関係者が、AI システム、ツール及びサービスだけではなく、モデルの訓練、モデルの再訓練、モデルの試験及び評価、ソフトウェアへの組み込み、または、それら以外の側面のモデルの開発を含め、様々な目的をもつ AI システムの中に提供者によって組み込まれているコンポーネントまたはプロセスも供給する。それらの関係者は、その関係者の AI システム、ツール、サービス、コンポーネントまたはプロセスが統合されている高リスク AI システムの提供者に向けられた価値連鎖の中で重要な役割をもつので、当該関係者自身の知的財産権または営業秘密を損なうことなく、この規則に定める義務を当該提供者が完全に遵守できるようにするため、

同提供者に対し、書面による合意により、必要な情報、実現能力、技術上のアクセス及びそれら以外の一般的に承認されている最新技術を基礎とする補助を提供すべきである。

Along the AI value chain multiple parties often supply AI systems, tools and services but also components or processes that are incorporated by the provider into the AI system with various objectives, including the model training, model retraining, model testing and evaluation, integration into software, or other aspects of model development. Those parties have an important role to play in the value chain towards the provider of the high-risk AI system into which their AI systems, tools, services, components or processes are integrated, and should provide by written agreement this provider with the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider to fully comply with the obligations set out in this Regulation, without compromising their own intellectual property rights or trade secrets.

- (89) 当該ツール、サービス、プロセスまたは AI コンポーネントが無料でオープンソースの使用許諾の下でアクセスできるようにされる場合、一般目的 AI モデル以外のツール、サービス、プロセスまたは AI コンポーネントを公衆に対して利用できるようにする第三者は、とりわけ、それらを使用または統合した提供者に向けた AI 価値連鎖の流れに沿った責任分担に的を絞っている要件を遵守することを義務づけられてはならない。一般目的 AI モデル以外の無料でオープンソースのツール、サービス、プロセスまたは AI コンポーネントの開発者は、欧州連合内における信頼できる AI システムの促進を可能にする、AI 価値連鎖の流れに沿った情報共有を加速させるための方途の 1 つとして、モデルカード及びデータシートのような、広く採用されている文書化実務を実装することが推奨されるべきである。

Third parties making accessible to the public tools, services, processes, or AI components other than general-purpose AI models, should not be mandated to comply with requirements targeting the responsibilities along the AI value chain, in particular towards the provider that has used or integrated them, when those tools, services, processes, or AI components are made accessible under a free and open-source licence. Developers of free and open-source tools, services, processes, or AI components other than general-purpose AI models should be encouraged to implement widely adopted documentation practices, such as model cards and data sheets, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the Union.

- (90) 欧州委員会は、価値連鎖の流れに沿った協力を容易にするため、高リスク AI システムの提供者と、高リスク AI システムの中で使用または統合されるツール、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の任意のモデル契約条項を策定し及び推奨し得る。任意のモデル契約条項を策定する際、欧州委員会は、個別の部門または取引事例において適用される可能性のある契約上の要件も考慮に入れるべきである。

The Commission could develop and recommend voluntary model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems, to facilitate the cooperation along the value chain. When developing voluntary model contractual terms, the Commission should also take into account possible contractual requirements applicable in specific sectors or business

cases.

- (91) AI システムの性質に鑑み、また、実世界の設定における AI システムの性能の適正な監視を確保することの必要性と関連するものを含め、AI システムの利用と関係して発生し得る安全及び基本的な権利に対するリスクに鑑み、設置者の個別の責任を定めることが適切である。とりわけ、設置者は、当該設置者が使用説明書に従って高リスク AI システムを利用することを確保するための適切な技術上及び組織上の方策をとるべきであり、また、その AI システムの稼働の監視と関連して、及び、記録の保存と関連して、上記以外の一定の義務がしかるべく定められるべきである。更に、設置者は、使用説明書及びこの規則に定める人間による監視を実装する役割を与えられた者が必要な能力をもつこと、とりわけ、その者の職務を適正に満たすための十分なレベルの AI リテラシ、訓練及び権限をもつことを確保すべきである。それらの義務は、欧州連合法または国内法の下における高リスク AI システムと関連する設置者の他の義務を妨げてはならない。

Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regards the need to ensure proper monitoring of the performance of an AI system in a *real-life* setting, it is appropriate to set specific responsibilities for deployers. Deployers should in particular take appropriate technical and organisational measures to ensure they use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate. Furthermore, deployers should ensure that the persons assigned to implement the instructions for use and human oversight as set out in this Regulation have the necessary competence, in particular an adequate level of AI literacy, training and authority to properly fulfil those tasks. Those obligations should be without prejudice to other deployer obligations in relation to high-risk AI systems under Union or national law.

- (92) この規則は、AI システムをサービスに供することまたはその利用の決定に関し、欧州議会及び理事会の指令 2002/14/EC³⁹を含め、欧州連合法または国内法及び実務に基づく使用者の情報提供の義務または使用者の労働者もしくは労働者の代表に対する情報提供及び意見聴取の義務を妨げない。他の法律文書の中にある同情報提供の条件または情報提供義務及び意見聴取義務が満たされていないときは、就労働場所における高リスク AI システムの設置予定に関して労働者及び労働者の代表に対する情報提供を確保することも必要なままである。それに加えて、そのような情報提供を受ける権利は、この規則の基盤となっている基本的な権利を保護するという目的のために補助的かつ必要である。それゆえ、労働者の既存の権利を損なうことなく、その効果をもつ情報提供の要件がこの規則の中で定められるべきである。

This Regulation is without prejudice to obligations for employers to inform or to inform and consult workers or their representatives under Union or national law and practice, including Directive 2002/14/EC of the European Parliament

³⁹ 欧州共同体内の従業者に対する情報提供及び意見聴取の一般的な枠組を設ける欧州議会及び理事会の 2002 年 3 月 11 日の指令 2002/14/EC (OJ L 80, 23.3.2002, p. 29).

Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community (OJ L 80, 23.3.2002, p. 29).

and of the Council⁽³⁹⁾, on decisions to put into service or use AI systems. It remains necessary to ensure information of workers and their representatives on the planned deployment of high-risk AI systems at the workplace where the conditions for those information or information and consultation obligations in other legal instruments are not fulfilled. Moreover, such information right is ancillary and necessary to the objective of protecting fundamental rights that underlies this Regulation. Therefore, an information requirement to that effect should be laid down in this Regulation, without affecting any existing rights of workers.

- (93) AI システムと関連するリスクは、そのようなシステムが設計された方法から生じ得るが、リスクは、そのような AI システムがどのように利用されるかからも派生し得る。それゆえ、高リスク AI システムの設置者は、基本的な権利が保護されることを確保する上で、及び、AI システムを開発する際における提供者の義務を補完する上で不可欠の役割を演ずる。設置者は、高リスク AI システムが具体的にどのように利用されることになるのかを理解するために最善のところに位置しており、それゆえ、利用の過程におけるより詳細な知識をもっているため、開発段階では想定されなかった潜在的な重大なリスクや、脆弱性のあるグループを含め、影響を受けるおそれのある個人または個人のグループを発見し得る。この規則の別紙の中に列挙される高リスク AI システムの設置者もまた、自然人に対する情報提供において重要な役割を演ずるのであり、当該設置者が自然人と関連する判定を行う場合、または、当該自然人と関連する判定を行う際の補助をする場合、それが適用可能なときは、その自然人に対し、その自然人が当該高リスク AI システムの利用に服していることを情報提供すべきである。この情報提供は、所期の目的及びそのシステムが行う判定のタイプを含めるべきである。設置者は、自然人に対し、その自然人のこの規則の下において提供される説明を受ける権利に関しても情報提供すべきである。法執行目的のために利用される高リスク AI システムに関しては、この義務は、指令(EU) 2016/680 の第 13 条に従って実装されるべきである。

Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the persons or groups of persons likely to be affected, including vulnerable groups. Deployers of high-risk AI systems listed in an annex to this Regulation also play a critical role in informing natural persons and should, when they make decisions or assist in making decisions related to natural persons, where applicable, inform the natural persons that they are subject to the use of the high-risk AI system. This information should include the intended purpose and the type of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided under this Regulation. With regard to high-risk AI systems used for law enforcement purposes, that obligation should be implemented in accordance with Article 13 of Directive (EU) 2016/680.

- (94) 法執行の目的のための生体要素識別のための AI システムの利用に含まれる生体要素データの処理は、データ主体の権利及び自由のための適切な安全確保に従い、厳格に必要な場合であり、かつ、欧州連合法または構成国法によって認められている場合に限り、そのような処理を許容する指令(EU) 2016/680 の第 10 条を遵守する必要がある。そのような利用は、それが認められるときは、適法

性、公正性及び透明性、目的の制限、正確性及び記録保存の制限を含め、指令(EU) 2016/680 の第 4 条第 1 項に定める基本原則も尊重する必要がある。

Any processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU) 2016/680, that allows such processing only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and where authorised by Union or Member State law. Such use, when authorised, also needs to respect the principles laid down in Article 4 (1) of Directive (EU) 2016/680 including lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

- (95) 適用可能な欧州連合法、とりわけ規則(EU) 2016/679 及び指令(EU) 2016/680 を妨げることなく、事後のリモート生体要素識別システムの侵害的な性質を考慮し、事後のリモート生体要素識別システムの利用は、安全確保に服するべきである。事後のリモート生体要素識別システムは、常に、比例的であり、適法であり、かつ、厳格に必要であり、そして、識別される個人、場所及び時間的範囲の面において的を絞った方法により、かつ、適法に得られたビデオ映像記録の非公開のデータセットを基礎として利用されるべきである。いかなる場合においても、事後のリモート生体要素識別システムは、無差別的な監視を導くために、法執行の枠組み内で利用されてはならない。事後のリモート生体要素識別の条件は、いかなる場合においても、リアルタイムのリモート生体要素識別に関する禁止及び厳格な適用除外の条件を回避するための根拠を提供してはならない。

Without prejudice to applicable Union law, in particular Regulation (EU) 2016/679 and Directive (EU) 2016/680, considering the intrusive nature of post-remote biometric identification systems, the use of post-remote biometric identification systems should be subject to safeguards. Post-remote biometric identification systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed data set of legally acquired video footage. In any case, post-remote biometric identification systems should not be used in the framework of law enforcement to lead to indiscriminate surveillance. The conditions for post-remote biometric identification should in any case not provide a basis to circumvent the conditions of the prohibition and strict exceptions for real time remote biometric identification.

- (96) 基本的な権利が保護されることを効率的に確保するため、公法によって規律される組織または公共サービスを提供する民間の運営者である高リスク AI システムの設置者、及び、銀行または保険機関のような、この規則の別紙の中に列挙される一定の高リスク AI システムの設置者は、そのシステムを利用に供する前に、基本的な権利の影響評価を実施すべきである。個人にとって重要な公共的な性質のサービスは、民間の法主体からも提供され得る。そのような公共的な性質のサービスを提供する民間の法主体は、教育、医療、社会サービス、住宅、法務上の行政の分野のような公共の利益における職務と結びついている。基本的な権利の影響評価の狙いは、設置者に関しては、影響を受けるおそれのある個人または個人のグループの権利に対する個別のリスクを識別すること、それらのリスクが現実化する場合においてとられるべき方策を見出すことである。影響評価は、当該高リスク AI システムが設置される前に遂行されるべきであり、かつ、関連する要素のいずれかが変化すると設置者が判断するときは、アップデートされるべきである。影響評価は、当該高リスク AI システムが所期

の目的に沿って利用されることになる当該設置者の関連プロセスを識別すべきであり、かつ、そのシステムが利用されることが意図されている期間及びその頻度、並びに、個別の利用の過程において影響を受けるおそれのある個別の種類の自然人及びグループの説明書を含めるべきである。評価は、それらの個人またはグループの基本的な権利に対して影響をもつおそれのある個別の危険のリスクの識別名も含めるべきである。この評価を遂行する際、設置者は、使用説明書の中で当該高リスク AI システムの提供者から与えられた情報を含め、かつ、その情報に限定されることなく、適切な影響評価と関連する情報を考慮に入れるべきである。識別されたリスクに照らし、設置者は、例えば、使用説明書に従った人間による監視の手立てのような、具体的な利用の過程における統治の手立てを含め、それらのリスクが現実化する場合にとられるべき方策を設計すべきであり、または、その手続が具体的な利用の場合における基本的な権利に対するリスクを緩和する上での道具であり得るので、苦情取扱い手続及び救済手続を決定すべきである。この影響評価の遂行の後、設置者は、関連する市場監視当局に対し、通知すべきである。それが適切なときは、影響評価を遂行するために必要な関連情報を収集するため、高リスク AI システムの設置者は、AI システムが公的部門で利用される場合においては特に、当該 AI システムによって影響を受けるおそれがある個人のグループの代表者、独立の専門家及び市民社会団体を含め、適格な利害関係者を、影響評価の遂行及びリスクの現実化の場合においてとられる方策の決定に含め得る。欧州人工知能総局(AI 総局)は、遵守を容易にし、かつ、設置者にかかる行政上の負担を削減するため、質問と回答の雛型を策定すべきである。

In order to efficiently ensure that fundamental rights are protected, deployers of high-risk AI systems that are bodies governed by public law, or private entities providing public services and deployers of certain high-risk AI systems listed in an annex to this Regulation, such as banking or insurance entities, should carry out a fundamental rights impact assessment prior to putting it into use. Services important for individuals that are of public nature may also be provided by private entities. Private entities providing such public services are linked to tasks in the public interest such as in the areas of education, healthcare, social services, housing, administration of justice. The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected, identify measures to be taken in the case of a materialisation of those risks. The impact assessment should be performed prior to deploying the high-risk AI system, and should be updated when the deployer considers that any of the relevant factors have changed. The impact assessment should identify the deployer's relevant processes in which the high-risk AI system will be used in line with its intended purpose, and should include a description of the period of time and frequency in which the system is intended to be used as well as of specific categories of natural persons and groups who are likely to be affected in the specific context of use. The assessment should also include the identification of specific risks of harm likely to have an impact on the fundamental rights of those persons or groups. While performing this assessment, the deployer should take into account information relevant to a proper assessment of the impact, including but not limited to the information given by the provider of the high-risk AI system in the instructions for use. In light of the risks identified, deployers should determine measures to be taken in the case of a materialisation of those risks, including for example governance arrangements in that specific context of use, such as arrangements for human oversight according to the instructions of use or, complaint handling and redress procedures, as they could be instrumental in mitigating risks to fundamental rights in concrete use-cases. After performing that impact assessment, the deployer should notify the relevant market surveillance authority. Where appropriate, to collect relevant

information necessary to perform the impact assessment, deployers of high-risk AI system, in particular when AI systems are used in the public sector, could involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations in conducting such impact assessments and designing measures to be taken in the case of materialisation of the risks. The European Artificial Intelligence Office (AI Office) should develop a template for a questionnaire in order to facilitate compliance and reduce the administrative burden for deployers.

- (97) 一般目的 AI モデルの概念は、明確に定義されるべきであり、かつ、法的確実性を実現可能にするため、AI システムの概念とは別に定められるべきである。その定義は、一般目的 AI モデルの鍵となる機能上の特性、とりわけ、幅広い異なる仕事を有能に遂行するための一般性と実現能力を基礎とすべきである。それらのモデルは、典型的には、自己監督あり学習、監督なし学習または強化学習のような様々な手法により、大量のデータを基礎とする訓練を受ける。一般目的 AI モデルは、ライブラリ、アプリケーションプログラミングインタフェース(APIs)を介する場合を含め、直接のダウンロードとして、または、物理的な複製物として、様々な方法で市場に置かれ得る。それらのモデルは、更に修正または微調整されて新たなモデルとなる。AI モデルが AI システムの必須のコンポーネントとなることがあるとしても、AI モデルは、それ自体としては AI システムを組成しない。AI システムとなるためには、AI モデルは、例えば、ユーザインタフェースのような更に別のコンポーネントの付加を必要とする。AI モデルは、典型的には、AI システムの中に統合されまたは AI システムの一部を形成する。この規則は、一般目的 AI モデルに関する細目的規定及びシステムリスクを呈する一般目的 AI モデルに関する細目的規定を定める。それらの規定は、当該モデルが AI システムの中に統合されまたは AI システムの一部を形成する場合にも適用されるべきである。一般目的 AI モデルの提供者の義務は、その一般目的 AI システムが市場に置かれた後に適用されるべきであるということが理解されるべきである。一般目的 AI システムの提供者が、市場に置かれているまたはサービスに供されているその提供者自身の AI システムに自身のモデルを統合する場合、当該モデルは市場に置かれていると判断されるべきであり、それゆえ、モデルに関するこの規則の義務は、AI システムに関する義務に付加して適用され続けるべきである。第三者に対して製品またはサービスを提供するために必須ではない純粋に内部的な処理のために自身のモデルが使用されており、かつ、自然人の権利が影響を受けないときは、いかなる場合においても、モデルに関して定められた義務を適用してはならない。システムリスクをもつ一般目的 AI モデルの潜在的に大きな負の影響を考慮し、システムリスクをもつ一般目的 AI モデルは、常に、この規則の下にある関連義務に服するべきである。定義条項は、調査研究、開発及びプロトタイプ活動の目的のみのために当該 AI モデルが市場に置かれる前に使用される AI モデルを包摂してはならない。このことは、そのような活動の後に、モデルが市場に置かれる際にはこの規則を遵守すべき義務を妨げない。

The notion of general-purpose AI models should be clearly defined and set apart from the notion of AI systems to enable legal certainty. The definition should be based on the key functional characteristics of a general-purpose AI model, in particular the generality and the capability to competently perform a wide range of distinct tasks. These models are typically trained on large amounts of data, through various methods, such as self-supervised, unsupervised or reinforcement learning. General-purpose AI models may be placed on the market in various ways, including through libraries, application programming interfaces (APIs), as direct download, or as physical copy. These models may be

further modified or fine-tuned into new models. Although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems. This Regulation provides specific rules for general-purpose AI models and for general-purpose AI models that pose systemic risks, which should apply also when these models are integrated or form part of an AI system. It should be understood that the obligations for the providers of general-purpose AI models should apply once the general-purpose AI models are placed on the market. When the provider of a general-purpose AI model integrates an own model into its own AI system that is made available on the market or put into service, that model should be considered to be placed on the market and, therefore, the obligations in this Regulation for models should continue to apply in addition to those for AI systems. The obligations laid down for models should in any case not apply when an own model is used for purely internal processes that are not essential for providing a product or a service to third parties and the rights of natural persons are not affected. Considering their potential significantly negative effects, the general-purpose AI models with systemic risk should always be subject to the relevant obligations under this Regulation. The definition should not cover AI models used before their placing on the market for the sole purpose of research, development and prototyping activities. This is without prejudice to the obligation to comply with this Regulation when, following such activities, a model is placed on the market.

- (98) モデルの一般性は、就中、多数のパラメータによって決定され得るものでもあるので、少なくとも 10 億のパラメータもち、かつ、自己監督学習を大規模に用い、大量のデータによって訓練されるモデルは、大きな一般性を示しており、かつ、幅広い異なる仕事を有能に遂行していると判断されるべきである。

Whereas the generality of a model could, inter alia, also be determined by a number of parameters, models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks.

- (99) 大規模な生成 AI モデルが、幅広い異なる仕事に容易に対応することができ、文、音響、画像または映像のような形態のコンテンツの柔軟な生成を許容することに鑑み、同モデルは、一般目的 AI モデルの典型的な例の 1 つである。

Large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks.

- (100) 一般目的 AI モデルが AI システムに統合されまたは AI システムの一部を形成する場合、そのシステムは、その組み込みのゆえにそのシステムが多様な目的に奉仕する実現能力をもつときは、一般目的 AI システムと判断されるべきである。一般目的 AI システムは、直接的に利用されることができ、また、別の AI システムの中に統合され得る。

When a general-purpose AI model is integrated into or forms part of an AI system, this system should be considered to be general-purpose AI system when, due to this integration, this system has the capability to serve a variety of purposes. A general-purpose AI system can be used directly, or it may be integrated into other AI systems.

- (101) 一般目的 AI モデルの提供者が提供するモデルが、当該モデルとそのモデルの実現能力の良好な理解を必要としている下流の提供者からしばしば提供される幅広い下流システムの基礎を形成することから、当該モデルの下流の提供者の製品への組み込みを実現可能にすること、並びに、この指令及び別の指令の下にある下流の提供者の義務を満たすことの両者のため、同モデルの提供者は、AI 価値連鎖の流れに沿った特別の役割と責任をもつ。それゆえ、文書を作成すること及び文書を最新の状態にすること並びに下流の提供者による一般目的 AI モデルの利用のための同モデルに関する情報の提供を含め、比例的な透明性の義務が定められるべきである。技術文書は、AI 総局及び職務権限のある国内機関に対して要求に応じて当該文書を利用できるようにする目的のために、一般目的 AI モデルの提供者によって準備されかつ最新の状態に保たれるべきである。そのような文書に含まれるべき要素のミニマムのセットは、この規則の個別の別紙の中で定められるべきである。欧州委員会は、進化する技術発展に照らし、委任される行為により、同別紙を改正する権限をもつべきである。

Providers of general-purpose AI models have a particular role and responsibility along the AI value chain, as the models they provide may form the basis for a range of downstream systems, often provided by downstream providers that necessitate a good understanding of the models and their capabilities, both to enable the integration of such models into their products, and to fulfil their obligations under this or other **regulations**. Therefore, proportionate transparency measures should be laid down, including the drawing up and keeping up to date of documentation, and the provision of information on the general-purpose AI model for its usage by the downstream providers. Technical documentation should be prepared and kept up to date by the general-purpose AI model provider for the purpose of making it available, upon request, to the AI Office and the national competent authorities. The minimal set of elements to be included in such documentation should be set out in **specific** annexes to this Regulation. The Commission should be empowered to amend those annexes by means of delegated acts in light of evolving technological developments.

- (102) モデルを含め、当該ソフトウェアとデータがオープンに共有されるようにし、かつ、利用者が当該ソフトウェアとデータに無料でアクセス、それを利用、修正でき、並びに、当該ソフトウェアとデータまたはその修正された版を再配布できる無料でオープンソースの使用許諾の下でリリースされるソフトウェアとデータは、市場における調査研究及び技術革新に寄与し得るのであり、また、欧州連合の経済にとって大きな成長の機会を提供し得る。無料でオープンソースの使用許諾の下においてリリースされる一般目的 AI モデルは、重みづけを含め、当該一般目的 AI モデルのパラメータ、モデルのアーキテクチャに関する情報及びモデルの利用に関する情報が公表されているときは、高いレベルの透明性及びオープン性を確保していると判断されるべきである。そのモデルの最初の提供者がクレジットされ、同一または同等の配布条件が尊重されるという条件の下にあるモデルを含め、利用者がソフトウェアとデータを実行、複製、配布、研究、変更及び改善することが許容されている場合においても、それらの使用許諾は、無料でオープンソースであると判断されるべきである。

Software and data, including models, released under a free and open-source licence that allows them to be openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market and can provide significant growth opportunities for the Union economy. General-purpose AI models released under free and open-source licences should be considered to ensure high levels of transparency and openness if their parameters, including the weights, the information on the model architecture, and the information on model usage are made publicly available. The licence should be considered to be free and open-source also when it allows users to run, copy, distribute, study, change and improve software and data, including models under the condition that the original provider of the model is credited, the identical or comparable terms of distribution are respected.

- (103) 無料でオープンソースの AI コンポーネントは、モデル及び一般目的 AI モデルを含め、AI システムのソフトウェアとデータ、ツール、サービスまたはプロセスを包摂する。無料でオープンソースの AI コンポーネントは、オープンナリポジトリ上におけるそのコンポーネントの開発を含め、異なる経路を通じて提供され得る。この規則の目的のために、マイクロ企業間におけるやりとりの場合を除き、ソフトウェアプラットフォームを介する場合を含めて AI コンポーネントと関連する技術上のサポートまたはそれ以外のサービスの提供を通じて行われる場合を含め、価格に応じて提供されまたはそれ以外の方法で収益化される AI コンポーネント、または、専らそのソフトウェアのセキュリティ、互換性もしくは相互運用性を改善するための場合以外の理由のための個人データの利用は、無料でオープンソースの AI コンポーネントに対して与えられる適用除外から受益してはならない。オープンナリポジトリを通じて AI コンポーネントを利用できるようにすることは、そのこと自体として、収益化を組成してはならない。

Free and open-source AI components covers the software and data, including models and general-purpose AI models, tools, services or processes of an AI system. Free and open-source AI components can be provided through different channels, including their development on open repositories. For the purposes of this Regulation, AI components that are provided against a price or otherwise monetised, including through the provision of technical support or other services, including through a software platform, related to the AI component, or the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, with the exception of transactions between **microenterprises**, should not benefit from the exceptions provided to free and open-source AI components. The fact of making AI components available through open repositories should not, in itself, constitute a monetisation.

- (104) 無料でオープンソースの使用許諾の下においてリリースされ、かつ、重みづけを含め、当該一般目的 AI モデルのパラメータ、モデルアーキテクチャに関する情報及びモデルの利用に関する情報が公表されている一般目的 AI モデルの提供者は、そのモデルがシステミックリスクを示していると判断され得ない限り、一般目的 AI モデルに対して課される透明性関連の要件に関する適用除外に服すべきである。そのモデルがシステミックリスクを示している場合、当該モデルに透明性がありかつオープンソースの使用許諾を伴っているという状況は、この規則の下にある義務の遵守を適用除外するための十分な根拠であると判断されてはならない。無料でオープンソースの使用許諾の下にある一般目的 AI モデルのリリースが、そのモデルの訓練または微調整のために使用されたデータセットに関する十分な情報及び著作権法の尊重がどのように確保されたかに関する十分な情報を明らか

にしているとは限らないことに鑑み、いかなる場合においても、透明性関連要件の遵守に関して定められる一般目的 AI モデルの適用除外は、モデルの訓練のために使用されたコンテンツに関する要旨を作成すべき義務、並びに、とりわけ欧州議会及び理事会の指令(EU) 2019/790⁴⁰の第 4 条第 3 項による権利の留保を識別し及び尊重するため、欧州連合の著作権法を尊重するための基本方針を設けるべき義務に関するものであってはならない。

The providers of general-purpose AI models that are released under a free and open-source licence, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available should be subject to exceptions as regards the transparency-related requirements imposed on general-purpose AI models, unless they can be considered to present a systemic risk, in which case the circumstance that the model is transparent and accompanied by an open-source license should not be considered to be a sufficient reason to exclude compliance with the obligations under this Regulation. In any case, given that the release of general-purpose AI models under free and open-source licence does not necessarily reveal substantial information on the data set used for the training or fine-tuning of the model and on how compliance of copyright law was thereby ensured, the exception provided for general-purpose AI models from compliance with the transparency-related requirements should not concern the obligation to produce a summary about the content used for model training and the obligation to put in place a policy to comply with Union copyright law, in particular to identify and comply with the reservation of rights pursuant to Article 4(3) of Directive (EU) 2019/790 of the European Parliament and of the Council⁽⁴⁰⁾.

- (105) 一般目的 AI モデル、とりわけ、文、画像及びそれ以外のコンテンツを生成する能力をもつ大規模な生成 AI モデルは、ユニークな技術革新の機会を提示するが、芸術家、著者及びそれ以外の創作者に対する検討課題並びにそれらの者の創造的なコンテンツが創作され、配布され、利用され及び消費される方法に対する検討課題も提示している。そのようなモデルの開発及び訓練は、膨大な分量の文、画像、映像及びそれ以外のデータへのアクセスを必要とする。文とデータの採掘技法は、著作権及び関連権によって保護されているかもしれないコンテンツの検索及び分析のために、そのようなコンテンツの検索及び分析の過程において拡張的に利用され得る。著作権保護のあるコンテンツの利用は、関連する著作権の適用除外及び制限が適用されない限り、関係する権利者の許諾を必要とする。指令(EU) 2019/790 は、一定の条件の下において、文及びデータの採掘の目的のために、作品またはそれ以外の対象の複製及び抽出をできるようにする適用除外と制限を導入した。それらの規定の下において、権利者は、それが科学の調査研究の目的のために行われるのでない限り、文及びデータの採掘を阻止するため、その権利者の作品またはそれ以外の対象に対するその権利者の権利を留保することを選択できる。適切な態様により撤回の権利が明示で留保されている場合、一般目的 AI モデルの提供者は、そのような作品を対象として文及びデータの採掘を実行することをその提供者が望むのであれば、権利者から許諾を得る必要がある。

⁴⁰ デジタル単一市場における著作権及び関連権に関する並びに指令 96/9/EC 及び指令 2001/29/EC を改正する欧州議会及び理事会の 2019 年 4 月 17 日の指令(EU)2019/790(OJ L 130, 17.5.2019, p.92).

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).

General-purpose AI models, in particular large generative AI models, capable of generating text, images, and other content, present unique innovation opportunities but also challenges to artists, authors, and other creators and the way their creative content is created, distributed, used and consumed. The development and training of such models require access to vast amounts of text, images, videos and other data. Text and data mining techniques may be used extensively in this context for the retrieval and analysis of such content, which may be protected by copyright and related rights. Any use of copyright protected content requires the authorisation of the rightsholder concerned unless relevant copyright exceptions and limitations apply. Directive (EU) 2019/790 introduced exceptions and limitations allowing reproductions and extractions of works or other subject matter, for the purpose of text and data mining, under certain conditions. Under these rules, rightsholders may choose to reserve their rights over their works or other subject matter to prevent text and data mining, unless this is done for the purposes of scientific research. Where the rights to opt out has been expressly reserved in an appropriate manner, providers of general-purpose AI models need to obtain an authorisation from rightsholders if they want to carry out text and data mining over such works.

- (106) 一般目的 AI モデルを欧州連合の市場に置く提供者は、この規則の中にある関連義務の遵守を確保すべきである。その目的のために、一般目的 AI モデルの提供者は、とりわけ、指令(EU) 2019/790 の第 4 条第 3 項によって権利者から表明される権利の留保を識別し及び尊重するため、著作権及び関連権に関する欧州連合法を尊重するための基本方針を設けるべきである。一般目的 AI モデルを EU の市場に置く提供者は、それらの一般目的 AI モデルの訓練を支えている著作権関連の行為が発生する地の裁判管轄権に拘わりなく、この義務を遵守すべきである。このことは、一般目的 AI モデルの提供者間における公平な競争の場を確保することを必要とする。その公平な競争の場においては、いかなる提供者も、欧州連合内において定められている著作権の基準よりも低い著作権の基準を適用することによって EU の市場内において競争上の優位を獲得できてはならない。

Providers that place general-purpose AI models on the Union market should ensure compliance with the relevant obligations in this Regulation. To that end, providers of general-purpose AI models should put in place a policy to comply with Union law on copyright and related rights, in particular to identify and comply with the reservation of rights expressed by rightsholders pursuant to Article 4(3) of Directive (EU) 2019/790. Any provider placing a general-purpose AI model on the Union market should comply with this obligation, regardless of the jurisdiction in which the copyright-relevant acts underpinning the training of those general-purpose AI models take place. This is necessary to ensure a level playing field among providers of general-purpose AI models where no provider should be able to gain a competitive advantage in the Union market by applying lower copyright standards than those provided in the Union.

- (107) 著作権法によって保護されている文及びデータを含め、一般目的 AI モデルの事前訓練及び訓練において利用されるデータの透明性を向上させるため、そのようなモデルの提供者が、その一般目的モデルの訓練のために利用したコンテンツの十分に詳細な要旨を作成しかつ公表することが適切である。営業秘密及び企業の機密情報を保護すべき必要性を適切に考慮に入れつつ、その要旨は、技術的に詳しく説明するのではなく、著作権者を含め正当な利益をもつ関係者が欧州連合法に下においてそれらの関係者の権利を行使及び執行することを容易にするため、例えば、民間または公的な大規模なデータベースまたはデータアーカイブのような、そのモデルの訓練において用いられた主なデータコレクションまたはデータセットを列挙することにより、及び、それら以外の利用された

データ資源に関するナラティブな説明を提供することにより、その要旨の適用範囲内において一般的に理解しやすいものであるべきである。AI 総局にとって、要旨のための雛型を提供することが適切である。その雛型は、簡素、実効的であるべきであり、かつ、要求される要旨をナラティブな方式によって当該提供者が提供できるようにするものであるべきである。

In order to increase transparency on the data that is used in the pre-training and training of general-purpose AI models, including text and data protected by copyright law, it is adequate that providers of such models draw up and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model. While taking into due account the need to protect trade secrets and confidential business information, this summary should be generally comprehensive in its scope instead of technically detailed to facilitate parties with legitimate interests, including copyright holders, to exercise and enforce their rights under Union law, for example by listing the main data collections or sets that went into training the model, such as large private or public databases or data archives, and by providing a **narrative** explanation about other data sources used. It is appropriate for the AI Office to provide a template for the summary, which should be simple, effective, and allow the provider to provide the required summary in **narrative** form.

- (108) 一般目的 AI モデルの提供者に課される、欧州連合の著作権法を尊重するための基本方針を設けるべき義務及び訓練に利用されたコンテンツの要旨を公表すべき義務に関し、AI 総局は、著作権の遵守の面における訓練データの仕事毎の評価を検証及び実施することなく、その提供者がそれらの義務を満したか否かを監視すべきである。この規則は、欧州連合法の下において定められている著作権規定の執行に影響を与えない。

With regard to the obligations imposed on providers of general-purpose AI models to put in place a policy to comply with Union copyright law and make publicly available a summary of the content used for the training, the AI Office should monitor whether the provider has fulfilled those obligations without verifying or proceeding to a work-by-work assessment of the training data in terms of copyright compliance. This Regulation does not affect the enforcement of copyright rules as provided for under Union law.

- (109) 一般目的 AI モデルの提供者に対して適用可能な義務の遵守は、それらの要件の任意の遵守がなお推奨されるべきであるとはいへ非職業上の目的または科学の調査研究の目的のためにモデルを開発または利用する者にとっての遵守の必要性の場合を除き、モデル提供者のタイプに対応して比例的であるべきである。欧州連合の著作権法を妨げることなく、それらの義務の遵守は、その提供者の規模を適正に考慮に入れるべきであり、かつ、スタートアップを含め SMEs のための簡素化された遵守方法を許容すべきであって、それは、費用負担が過剰であることを示してはならず、かつ、そのようなモデルの利用を断念させてはならない。モデルの修正または微調整の場合、一般目的 AI モデルの提供者の義務は、この規則に定める価値連鎖の義務を遵守するための手段として、例えば、新たな訓練データ資源を含め、修正に関する情報により既存の技術文書を補完することによって、当該修正または微調整に限定されるべきである。

Compliance with the obligations applicable to the providers of general-purpose AI models should be commensurate and proportionate to the type of model provider, excluding the need for compliance for persons who develop or use

models for non-professional or scientific research purposes, who should nevertheless be encouraged to voluntarily comply with these requirements. Without prejudice to Union copyright law, compliance with those obligations should take due account of the size of the provider and allow simplified ways of compliance for SMEs, including start-ups, that should not represent an excessive cost and not discourage the use of such models. In the case of a modification or fine-tuning of a model, the obligations for providers of general-purpose AI models should be limited to that modification or fine-tuning, for example by complementing the already existing technical documentation with information on the modifications, including new **training data sources**, as a means to comply with the value chain obligations provided in this Regulation.

- (110) 一般目的 AI モデルは、システムリスクを呈し得る。そのシステムリスクは、重大事故、不可欠部門の混乱及び公衆の健康と安全に対する重大な結果と関係する現実の負の影響または合理的に予測可能な負の影響; 民主的な過程、公共の保安及び経済安全保障に対する現実の負の影響または合理的に予測可能な負の影響; 違法なコンテンツ、虚偽のコンテンツまたは差別的なコンテンツの流通を含むが、それらに限定されない。システムリスクは、モデルの実現能力及びモデルの利用者数に応じて増加するということが理解されるべきであり、当該モデルの全ライフサイクルに沿って生じ得るのであり、そして、濫用の諸条件、モデルの信頼性、モデルの公正性及びモデルのセキュリティ、モデルの自律性のレベル、当該モデルのツールへのアクセス、新規のモダリティまたは複合的モダリティ、リリース戦略と流通戦略、ガードレールを除去する潜在力及びそれら以外の要素による影響を受ける。とりわけ、国際的なアプローチは、これまで、潜在的で意図的な濫用または人間の意図と揃えることと関連する意図的でない管理上の問題からのリスク; 武器の開発、設計、獲得または利用のための場合を含め、参入の障壁が低くされ得る方法のような、化学のリスク、生物学的なリスク、放射線及び核のリスク; 脆弱性の発見、悪用または作戦上の利用が実現され得るようにする方法のような攻撃的なサイバー能力; 例えば、物理システムを支配するための能力及び不可欠インフラを妨害するための能力を含め、やりとり及びツールの利用の影響; 自身の複製物の製造のモデルもしくは「自己複製」のモデルまたは他のモデルを訓練するモデルからのリスク; 個人、コミュニティまたは社会に対するリスクのある危険なバイアス及び差別を当該モデルが生じさせ得る方法; 民主主義の価値及び人権に対する脅威をもつ偽情報の促進またはプライバシーの危殆化; ある個別の出来事が、都市全体、ある分野の活動全体またはコミュニティ全体にまで影響を及ぼし得る重大な負の影響をもつ連鎖的な反作用を導き得るリスクに対して注意を払う必要性を識別してきた。

General-purpose AI models could pose systemic risks which include, but are not limited to, any actual or reasonably foreseeable negative effects in relation to major accidents, disruptions of critical sectors and serious consequences to **public health and safety**; any actual or reasonably foreseeable negative effects on democratic processes, public and economic security; the dissemination of illegal, false, or discriminatory content. Systemic risks should be understood to increase with model capabilities and model reach, can arise along the entire lifecycle of the model, and are influenced by conditions of misuse, model reliability, model fairness and model security, the level of autonomy of the model, its access to tools, novel or combined modalities, release and distribution strategies, the potential to remove guardrails and other factors. In particular, international approaches have so far identified the need to pay attention to risks from potential intentional misuse or unintended issues of control relating to alignment with human intent; chemical, biological, radiological, and nuclear risks, such as the ways in which barriers to entry can be lowered, including for weapons

development, **design acquisition**, or use; offensive cyber capabilities, such as the ways in which vulnerability discovery, exploitation, or operational use can be enabled; the effects of interaction and tool use, including for example the capacity to control physical systems and interfere with critical infrastructure; risks from models of making copies of themselves or ‘self-replicating’ or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event could lead to a chain reaction with considerable negative effects that could affect up to an entire city, an entire domain activity or an entire community.

- (111) システミックリスクをもつ一般目的 AI モデルとして一般目的 AI モデルを分類するための手法を確立することが適切である。システミックリスクは特段に高度な実現能力から生ずるので、一般目的 AI モデルは、そのモデルが、適切な技術ツール及び手法を基礎として評価された高い影響力のある実現能力をもち、または、その利用者数のゆえの域内市場に対する大きな影響をもつときは、システミックリスクを示すものと判断されるべきである。一般目的 AI モデルにおける高い影響力をもつ実現能力とは、最高度の一般目的 AI モデルにおいて記録された実現能力と一致またはそれを超過する実現能力のことを意味する。あるモデルにおける実現能力の最大限度は、当該モデルを市場に置いた後において、または、設置者がモデルとの間でやりとりする際により良く理解され得る。この規則の発効の時点における最新技術に従い、浮動小数点演算において測定された一般目的 AI モデルの訓練のために使用された計算の積算量は、モデルの実現能力と関連する近似値の 1 つである。訓練のために使用された計算量は、事前訓練、合成データの生成及び微調整のような、設置に先立ってそのモデルの実現能力を拡大することを意図する活動及び手法の全体にわたり使用された計算を積算する。それゆえ、浮動小数点演算の最初の閾値が設定されるべきである。その閾値は、もし一般目的 AI モデルがそれに適合するのであれば、当該モデルがシステミックリスクをもつ一般目的 AI モデルであるということの推定を導く。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向上のような技術上及び産業上の変化を反映するため、時の経過とともに補正されるべきであり、また、モデルの実現能力のベンチマーク及び指標によって補完されるべきである。このことを情報提供するため、AI 総局は、科学のコミュニティ、産業界、市民社会団体及びそれら以外の専門家と関わりをもつべきである。高い影響力をもつ実現能力の評価のための閾値並びにツール及びベンチマークは、一般目的 AI モデルの一般性、実現能力及び関連するシステミックリスクの強力な予測因子であるべきであり、かつ、当該モデルが市場に置かれる方法及び影響を受け得る利用者の数を考慮に入れ得る。この方式を補完するため、設定された閾値によって把握される実現能力または影響と均等な実現能力または影響をそのようなモデルがもつと欧州委員会が判断するときは、欧州委員会は、システミックリスクをもつ一般目的 AI モデルとして一般目的 AI モデルを指定する個別の判定を行う可能性が存在するべきである。その判定は、訓練データセットの品質または規模、企業ユーザ及びエンドユーザの数、そのモデルの入力モダリティ及び出力モダリティ、そのモデルの自律性及び拡張性の程度、または、そのモデルがアクセスしたツールのような、この規則の別紙の中で定められるシステミックリスクをもつ一般目的 AI モデルの指定のために基準の評価全体を基礎として行われるべきである。その者のモデルがシステミックリスクをもつ一般目的 AI モデルとして指定された提供者の理由を付した求めがあるときは、欧州委員会は、その求めを考慮に入れるべきであり、かつ、その一般目的 AI モデルがシステミックリスクを示しているとの判断を維持し得るかどうかを見直す決定を行い得る。

It is appropriate to establish a methodology for the classification of general-purpose AI models as general-purpose AI model with systemic risks. Since systemic risks result from particularly high capabilities, a general-purpose AI model should be considered to present systemic risks if it has high-impact capabilities, evaluated on the basis of appropriate technical tools and methodologies, or significant impact on the internal market due to its reach. High-impact capabilities in general-purpose AI models means capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models. The full range of capabilities in a model could be better understood after its placing on the market or when deployers interact with the model. According to the state of the art at the time of entry into force of this Regulation, the cumulative amount of computation used for the training of the general-purpose AI model measured in floating point operations is one of the relevant approximations for model capabilities. The cumulative amount of computation used for training includes the computation used across the activities and methods that are intended to enhance the capabilities of the model prior to deployment, such as pre-training, synthetic data generation and fine-tuning. Therefore, an initial threshold of floating point operations should be set, which, if met by a general-purpose AI model, leads to a presumption that the model is a general-purpose AI model with systemic risks. This threshold should be adjusted over time to reflect technological and industrial changes, such as algorithmic improvements or increased hardware efficiency, and should be supplemented with benchmarks and indicators for model capability. To inform this, the AI Office should engage with the scientific community, industry, **civil society** and other experts. Thresholds, as well as tools and benchmarks for the assessment of high-impact capabilities, should be strong predictors of generality, **its** capabilities and associated systemic risk of general-purpose AI models, and could take into account the way the model will be placed on the market or the number of **users** it may affect. To complement this system, there should be a possibility for the Commission to take individual decisions designating a general-purpose AI model as a general-purpose AI model with systemic risk if it is found that such model has capabilities or an impact equivalent to those captured by the set threshold. That decision should be taken on the basis of an overall assessment of the criteria for the designation of a general-purpose AI model with systemic risk set out in an annex to this Regulation, such as quality or size of the **training data set**, number of business and end users, its input and output modalities, its level of autonomy and scalability, or the tools it has access to. Upon a reasoned request of a provider whose model has been designated as a general-purpose AI model with systemic risk, the Commission should take the request into account and may decide to reassess whether the general-purpose AI model can still be considered to present systemic risks.

- (112) システミックリスクをもつ一般目的 AI モデルの分類のための手続を明確にすることも必要である。高い影響力をもつ実現能力に関する適用可能な閾値に適合する一般目的 AI モデルは、システミックリスクをもつ一般目的 AI モデルであると推定されるべきである。その提供者は、AI 総局に対し、その要件に適合した後、または、一般目的 AI モデルが同推定を導く要件に適合することになるということを知った後、遅くとも 2 週間以内に通知すべきである。一般目的 AI モデルの訓練では計算資源の事前の割当てを含む大規模な計画検討を行い、それゆえ、当該訓練が完了する前に当該提供者のモデルが閾値に適合するかどうかを一般目的 AI モデルの提供者が知り得るので、この通知は、浮動小数点演算の閾値との関係において特に関連性をもつ。この通知の過程において、提供者は、そのモデルの個別の特性を理由として、一般目的 AI モデルが例外的にシステミックリスクを示しておらず、そのモデルがシステミックリスクをもつ一般目的 AI モデルとして分類されてはならないことを示すことができるべきである。この情報提供は、システミックリスクをもつ一般目的 AI モデルが市場に置かれることを予測するために AI 総局にとって価値があり、また、提供者は、早い段階で AI 総局と

の間でかわりをもつことを開始できる。オープンソースのモデルのリリース後においては、この規則の下にある義務の遵守を確保するために必要となる措置が一層実装困難になるかもしれないことに鑑み、オープンソースとしてリリースされることが計画されている一般目的 AI モデルに関しては、この情報提供は、とりわけ重要である。

It is also necessary to clarify a procedure for the classification of a general-purpose AI model with systemic risks. A general-purpose AI model that meets the applicable threshold for high-impact capabilities should be presumed to be a general-purpose AI model with systemic risk. The provider should notify the AI Office at the latest two weeks after the requirements are met or it becomes known that a general-purpose AI model will meet the requirements that lead to the presumption. This is especially relevant in relation to the threshold of floating point operations because training of general-purpose AI models takes considerable planning which includes the upfront allocation of compute resources and, therefore, providers of general-purpose AI models are able to know if their model would meet the threshold before the training is completed. In the context of that notification, the provider should be able to demonstrate that, because of its specific characteristics, a general-purpose AI model exceptionally does not present systemic risks, and that it thus should not be classified as a general-purpose AI model with systemic risks. That information is valuable for the AI Office to anticipate the placing on the market of general-purpose AI models with systemic risks and the providers can start to engage with the AI Office early on. That information is especially important with regard to general-purpose AI models that are planned to be released as open-source, given that, after the open-source model release, necessary measures to ensure compliance with the obligations under this Regulation may be more difficult to implement.

- (113) 一般目的 AI モデルがシステミックリスクをもつ一般的な目的をもつ AI モデルとして分類するための要件に適合するものであって、そのことが従前には知られていなかったこと、または、関連する提供者が欧州委員会に対して通知しなかったことに欧州委員会が気付いたときは、欧州委員会は、そのように指定するための権限を与えられるべきである。該当性あり警報の制度は、AI 総局の監視活動に加え、一般目的 AI モデルの科学パネルによって、システミックリスクをもつ一般目的 AI モデルとして分類される可能性があることに AI 総局が気付くことを確保すべきである。

If the Commission becomes aware of the fact that a general-purpose AI model meets the requirements to classify as a general-purpose AI model with systemic risk, which previously had either not been known or of which the relevant provider has failed to notify the Commission, the Commission should be empowered to designate it so. A system of qualified alerts should ensure that the AI Office is made aware by the scientific panel of general-purpose AI models that should possibly be classified as general-purpose AI models with systemic risk, in addition to the monitoring activities of the AI Office.

- (114) システミックリスクをもつ一般目的 AI モデルの提供者は、一般目的 AI モデルの提供者に関して定められた義務に加え、そのモデルがスタンドアロンのモデルとして提供されるか AI システムもしくは製品の中に組み込まれるかに拘わらず、当該システミックリスクを識別すること及び緩和すること並びに十分なレベルのサイバーセキュリティ上の保護を確保することを狙いとする義務に服すべきである。それらの目的を達成するため、この規則は、提供者に対し、とりわけ当該 AI モデルを最初に市場に置く前に、モデルの敵対的試験の実施及び文書化を含め、また、それが適切なときは、内部試

験または独立の外部試験により、必要なモデル評価を遂行することを要求すべきである。加えて、システミックリスクをもつ一般目的 AI モデルの提供者は、例えば、説明責任や統治のプロセスのようなリスク管理の基本方針を設けること、市場化後監視を実装すること、モデルの全ライフサイクルの流れに沿って適切な方策をとること、及び、AI 価値連鎖の流れに沿って適格な関与者と協力することによる場合を含め、システミックリスクを継続的に評価し、かつ、それを緩和すべきである。

The providers of general-purpose AI models presenting systemic risks should be subject, in addition to the obligations provided for providers of general-purpose AI models, to obligations aimed at identifying and mitigating those risks and ensuring an adequate level of cybersecurity protection, regardless of whether it is provided as a standalone model or embedded in an AI system or a product. To achieve those objectives, this Regulation should require providers to perform the necessary model evaluations, in particular prior to its first placing on the market, including conducting and documenting adversarial testing of models, also, as appropriate, through internal or independent external testing. In addition, providers of general-purpose AI models with systemic risks should continuously assess and mitigate systemic risks, including for example by putting in place risk-management policies, such as accountability and governance processes, implementing post-market monitoring, taking appropriate measures along the entire model's lifecycle and cooperating with relevant actors along the AI value chain.

- (115) システミックリスクをもつ一般目的 AI モデルの提供者は、あり得るシステミックリスクを評価し、かつ、それを緩和すべきである。システミックリスクを示すかもしれない一般目的 AI モデルと関連するリスクを識別するため及びそれを防止するための努力にも拘わらず、そのモデルの開発または利用が重大なインシデントを発生させるときは、その一般目的 AI モデルの提供者は、不適切な遅滞なく、そのインシデントの追跡を維持し、かつ、欧州委員会及び職務権限のある国内機関に対し、関連情報及び可能な是正の方策を報告すべきである。更に、提供者は、それが適切なときはそのモデルの全ライフサイクルの流れに沿って、そのモデル及びそのモデルの物理インフラのための十分なレベルのサイバーセキュリティ上の保護を確保すべきである。悪意ある利用または攻撃と関係するシステミックリスクに関するサイバーセキュリティ上の保護は、偶発的なモデルの漏洩、未承認のリリース、安全性の方策の回避、及び、サイバー攻撃、無権限アクセスまたはモデルの盗取に抗する防御を適正に検討すべきである。この保護は、情報セキュリティのための業務運営上の防護の方策、サイバーセキュリティ上の個別の基本方針、技術上の確立された適切なリニューション、サイバーなアクセス管理及び物理的なアクセス管理による場合のように、関連する状況及び包摂されているリスクに応じて適切な、モデルの重みづけ、アルゴリズム、サーバ及びデータセットを防護することによって促進され得る。

Providers of general-purpose AI models with systemic risks should assess and mitigate possible systemic risks. If, despite efforts to identify and prevent risks related to a general-purpose AI model that may present systemic risks, the development or use of the model causes a serious incident, the general-purpose AI model provider should **without undue delay** keep track of the incident and report any relevant information and possible corrective measures to the Commission and national competent authorities. Furthermore, providers should ensure an adequate level of cybersecurity protection for the model and its physical infrastructure, if appropriate, along the entire model lifecycle. Cybersecurity protection related to systemic risks associated with malicious use or attacks should duly consider accidental model leakage, unauthorised releases, circumvention of safety measures, and defence against cyberattacks,

unauthorised access or model theft. That protection could be facilitated by securing model weights, algorithms, servers, and data sets, such as through operational security measures for information security, specific cybersecurity policies, adequate technical and established solutions, and cyber and physical access controls, appropriate to the relevant circumstances and the risks involved.

- (116) AI 総局は、国際的なアプローチを考慮に入れた上で、実務準則の作成、見直し及び調整を推進及び促進すべきである。一般目的 AI モデルの全ての提供者は、参加を招請され得る。実務準則が最新技術を反映すること及び多様なセクトの将来展望を適正に考慮に入れることを確保するため、AI 総局は、適切な職務権限のある国内機関と共働すべきであり、また、そのような準則を作成するため、それが適切なときは、市民社会団体及びそれ以外の適格な利害関係者、並びに、科学パネルを含め、専門家の意見を聴取し得る。実務準則は、一般目的 AI モデルの提供者及びシステムリスクをもつ一般目的 AI モデルの提供者に関する義務を包摂する。加えて、システムリスクに関し、実務準則は、システムリスクの発生源を含め、システムリスクのタイプ及び性質のリスク分類を欧州連合レベルで確立することを助けるべきである。実務準則は、個別のリスク評価及び緩和方策に対しても焦点を当てるべきである。

The AI Office should encourage and facilitate the drawing up, review and adaptation of codes of practice, taking into account international approaches. All providers of general-purpose AI models could be invited to participate. To ensure that the codes of practice reflect the state of the art and duly take into account a diverse set of perspectives, the AI Office should collaborate with relevant national competent authorities, and could, where appropriate, consult with civil society organisations and other relevant stakeholders and experts, including the Scientific Panel, for the drawing up of such codes. Codes of practice should cover obligations for providers of general-purpose AI models and of general-purpose AI models presenting systemic risks. In addition, as regards systemic risks, codes of practice should help to establish a risk taxonomy of the type and nature of the systemic risks at Union level, including their sources. Codes of practice should also be focused on specific risk assessment and mitigation measures.

- (117) 実務準則は、一般目的 AI モデルの提供者に関するこの規則の下において定められる義務の適正な遵守のための中心的なツールを表すべきである。提供者は、義務の遵守を説明するために実務準則に依拠できるべきである。欧州委員会は、実装行為により、実務準則を承認し、かつ、その実務準則に対して欧州連合内における一般的な有効性を与えること、または、この規則が適用可能となる時までに行動準則が完成されていないとき、もしくは、AI 総局によって十分ではないと判定されるときは、代替として、関連する義務の実装のための共通規定を定めることを決定できる。整合化された技術標準が公示され、かつ、AI 総局によって関連義務に適用するために適切であると評価された後は、欧州の整合化された技術標準の遵守は、提供者に対し、適合性の推定を与えるべきである。更に、一般目的 AI モデルの提供者は、実務準則もしくは整合化された技術標準が利用できない場合、または、それらに依拠することをその提供者が選択しない場合においては、適切な代替手段を用いて遵守を説明できるべきである。

The codes of practice should **represent** a central tool for the proper compliance with the obligations provided for under this Regulation for providers of general-purpose AI models. Providers should be able to rely on codes of practice to demonstrate compliance with the obligations. By means of implementing acts, the Commission may decide to approve

a **code of practice** and give it a general validity within the Union, or, alternatively, to provide common rules for the implementation of the relevant obligations, if, by the time this Regulation becomes applicable, a **code of practice** cannot be finalised or is not deemed adequate by the AI Office. Once a harmonised standard is published and assessed as suitable to cover the relevant obligations by the AI Office, compliance with a European harmonised standard should grant providers the presumption of conformity. Providers of general-purpose AI models should furthermore be able to demonstrate compliance using alternative adequate means, if codes of practice or harmonised standards are not available, or they choose not to rely on those.

- (118) この規則は、欧州連合内において AI システムを市場に置いており、サービスに供してありまたは利用する関連市場の関与者に対して一定の要件及び義務を課すことによって、そして、それによって、規則(EU) 2022/2065 によって規律されるそれらのサービスの中にそのようなシステムまたはモデルを組み込む中間介在サービスの提供者の義務を補完することにより、AI システム及び AI モデルを規律する。指定された非常に大きなオンラインプラットフォームまたは非常に大きなオンライン検索エンジンの中にそのようなシステムまたはモデルが組み込まれている範囲内において、それらのシステムまたはモデルは、規則(EU) 2022/2065 に定めるリスク管理の枠組みに服する。その結果として、規則(EU) 2022/2065 の適用を受けない重大なシステムリスクがそのようなモデルの中で発生しかつ識別されない限り、この規則の対応する義務が満たされていると推定されるべきである。この枠組みの範囲内において、非常に大きなオンラインプラットフォームのプロバイダ及び非常に大きなオンライン検索エンジンのプロバイダは、そのサービスの中で使用されているアルゴリズム体系の設計がどのようにそのようなリスクに寄与しているか、及び、潜在的な濫用から派生するシステムリスクを含め、当該プロバイダのサービスの設計、稼働及び利用から派生する潜在的なシステムリスクを評価することを義務づけられる。それらのプロバイダは、基本的な権利を尊重して、適切な緩和の方策をとることも義務づけられる。

This Regulation regulates AI systems and AI models by imposing certain requirements and obligations for relevant market actors that are placing them on the market, putting into service or use in the Union, thereby complementing obligations for providers of intermediary services that embed such systems or models into their services regulated by Regulation (EU) 2022/2065. To the extent that such systems or models are embedded into designated very large online platforms or very large online search engines, they are subject to the risk-management framework provided for in Regulation (EU) 2022/2065. Consequently, the corresponding obligations of this Regulation should be presumed to be fulfilled, unless significant systemic risks not covered by Regulation (EU) 2022/2065 emerge and are identified in such models. Within this framework, providers of very large online platforms and very large online search engines are obliged to assess potential systemic risks stemming from the design, functioning and use of their services, including how the design of algorithmic systems used in the service may contribute to such risks, as well as systemic risks stemming from potential misuses. Those providers are also obliged to take appropriate mitigating measures in observance of fundamental rights.

- (119) 技術革新の速いペース及び欧州連合法の異なる法律文書の適用範囲内にあるデジタルサービスの技術的な進化を考慮し、とりわけ、その利用及びその受け手の知覚を念頭に置いて、この規則に服する AI システムは、規則(EU) 2022/2065 の意味における中間介在サービスまたはその一部として

提供され得る。それは、技術的に中立な態様で解釈されるべきである。例えば、AI システムは、とりわけ、オンラインチャットボットのような AI システムが原則として全ての Web サイトの検索を遂行し、そして、その結果を当該 AI システムの知識の中に組み込み、また、異なる情報源の情報を束ねる単一の出力を生成するためにアップデートされた知識を利用する範囲内において、オンライン検索エンジンを提供するために利用され得る。

Considering the quick pace of innovation and the technological evolution of digital services in scope of different instruments of Union law in particular having in mind the usage and the perception of their recipients, the AI systems subject to this Regulation may be provided as intermediary services or parts thereof within the meaning of Regulation (EU) 2022/2065, which should be interpreted in a technology-neutral manner. For example, AI systems may be used to provide online search engines, in particular, to the extent that an AI system such as an online chatbot performs searches of, in principle, all websites, then incorporates the results into its existing knowledge and uses the updated knowledge to generate a single output that combines different sources of information.

- (120) 更に、当該システムの出力が人工的に生成または操作されていることの検出及び開示を実現可能とするためにこの規則の中で一定の AI システムの提供者及び設置者に対して課される義務は、規則 (EU) 2022/2065 の実効的な実装を容易にすることと特に関連している。このことは、とりわけ、非常に大きなオンラインプラットフォームのプロバイダまたは非常に大きなオンライン検索エンジンのプロバイダの義務と関連して、人工的に生成または操作されたコンテンツの流通から生じ得るシステムリスク、とりわけ、偽情報による場合を含め、民主的な過程、市民の意見交換と選挙のプロセスに対する現実のまたは予測可能な負の影響というリスクを識別し及びそれを緩和するために適用される。

Furthermore, obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.

- (121) 標準化は、最新の技術に沿ってこの規則の遵守を確保するため、単一市場内における技術革新並びに競争力及び成長を促進するため、提供者に対して技術上のソリューションを提供するための鍵となる役割を果たすべきである。欧州議会及び理事会の規則 (EU) No 1025/2012⁴¹ の第 2 条第 1 号(c) の中で定義されており、通常は最新技術を反映していることが期待される整合化された技術標準の遵守は、提供者がこの規則の要件の遵守を説明するための手段の 1 つであるべきである。それゆえ、技術標準の策定に関与する全ての適格な利害関係者の利益、とりわけ、SMEs、消費者団体並びに環境上及び社会上の利害関係者の利益が規則 (EU) No 1025/2012 の第 5 条及び第 6 条に従ってバランス良く反映されることが推進されるべきである。遵守を容易にするため、標準化の要請は、不適切な遅滞なく、欧州委員会から発されるべきである。標準化の要請を準備する際、欧州委員会は、関連する専門知識を収集するため、諮問フォーラム及び委員会の意見を聴取すべきである。ただし、

整合化された技術標準と関連する参照が存在しないときは、欧州委員会は、実装行為により、かつ、諮問フォーラムからの意見聴取の後、この規則の下における一定の要件に関する共通仕様を定め得るべきである。標準化を求める要請が欧州の標準化組織によって受諾されなかった場合、または、関連する整合化された技術標準が関係する基本的な権利の懸念に十分に対処していない場合、または、整合化された技術標準が当該要請を遵守していない場合、または、適切な整合化された技術標準の採択に遅延がある場合、その共通仕様は、この規則の要件を遵守すべき提供者の義務を容易にするための例外的なフォールバックソリューションの 1 つであるべきである。整合化された技術標準の採択におけるそのような遅延が当の技術標準の技術上の複雑性によるものである場合、そのことは、共通仕様の策定を検討する前に、欧州委員会によって検討されるべきである。共通仕様を策定する際、欧州委員会は、国際的な関係者及び国際的な標準化組織と協力することが推奨される。

Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation, in line with the state of the art, to promote innovation as well as competitiveness and growth in the single market. Compliance with harmonised standards as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council⁴¹, which are normally expected to reflect the state of the art, should be a means for providers to demonstrate conformity with the requirements of this Regulation. A balanced representation of interests involving all relevant stakeholders in the development of standards, in particular SMEs, consumer organisations and environmental and social stakeholders in accordance with Articles 5 and 6 of Regulation (EU) No 1025/2012 should therefore be encouraged. In order to facilitate compliance, the standardisation requests should be issued by the Commission without undue delay. When preparing the standardisation request, the Commission should consult the advisory forum and the Board in order to collect relevant expertise. However, in the absence of relevant references to harmonised standards, the Commission should be able to establish, via implementing acts, and after consultation of the advisory forum, common specifications for certain requirements under this Regulation. The common specification should be an exceptional fall back solution to facilitate the provider's obligation to comply with the requirements of this Regulation, when the standardisation request has not been accepted by any of the European standardisation organisations, or when the relevant harmonised standards insufficiently address fundamental rights concerns, or when the harmonised standards do not comply with the request, or when there are delays in the adoption of an appropriate harmonised standard. Where such a delay in the adoption of a harmonised standard is due to the technical complexity of that standard, this should be considered by the Commission before contemplating the establishment of common specifications. When developing common specifications, the Commission is encouraged to cooperate with international partners and international standardisation bodies.

⁴¹ 欧州の標準化に関する、理事会指令 89/686/EEC 及び理事会指令 93/15/EEC、欧州議会及び理事会の指令 94/9/EC、指令 94/25/EC、指令 95/16/EC、指令 97/23/EC、指令 98/34/EC、指令 2004/22/EC、指令 2007/23/EC、指令 2009/23/EC 及び指令 2009/105/EC を改正し、理事会決定 87/95/EEC、欧州議会及び理事会の決定 No 1673/2006/EC を廃止する欧州議会及び理事会の 2012 年 10 月 25 日の規則(EU)No 1025/2012(OJL316, 14.11.2012, p. 12).

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJL316, 14.11.2012, p. 12).

- (12) 整合化された技術標準及び共通仕様の利用を妨げることなく、その AI システムが利用されることが意図されている範囲内における個別の地理的設定、行動上の設定、文脈上の設定または機能上の設定を反映してデータが訓練され及び試験された高リスク AI システムの提供者は、この規則に定めるデータ統治に関する要件の下において定められている関連措置を遵守していると推定されるべきである。この規則に定める堅牢性及び正確と関係する要件を妨げることなく、規則(EU) 2019/881 の第 54 条第 3 項に従い、同規則によるサイバーセキュリティ制度の下において認証を受けまたはそのシステムに関して適合性宣言書が発行され、かつ、EU 官報上でそのシステムの参照が公示された高リスク AI システムは、そのサイバーセキュリティ認証もしくは適合性宣言書またはその一部がこの規則のサイバーセキュリティ上の要件を包摂している範囲内において、この規則のサイバーセキュリティ上の要件を遵守していると推定されるべきである。このことは、同サイバーセキュリティ制度の任意という性質を妨げないままである。

It is appropriate that, without prejudice to the use of harmonised standards and common specifications, providers of a high-risk AI system that has been trained and tested on data reflecting the specific geographical, behavioural, contextual or functional setting within which the AI system is intended to be used, should be presumed to comply with the relevant measure provided for under the requirement on data governance set out in this Regulation. Without prejudice to the requirements related to robustness and accuracy set out in this Regulation, in accordance with Article 54(3) of Regulation (EU) 2019/881, high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to that Regulation and the references of which have been published in the *Official Journal of the European Union* should be presumed to comply with the cybersecurity requirement of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover the cybersecurity requirement of this Regulation. This remains without prejudice to the voluntary nature of that cybersecurity scheme.

- (123) 高リスク AI システムの高いレベルの信頼性を確保するため、それらのシステムは、そのシステムが市場に置かれまたはサービスに供される前に、適合性評価に服するべきである。

In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.

- (124) 運用者の負担をミニマム化するため、及び、あり得る重複を避けるため、新たな立法枠組みを基礎とする現行の欧州連合整合化立法が適用される製品と関連する高リスク AI システムに関しては、それらの AI システムのこの規則の要件の遵守は、当該法律の下において既に定められている適合性評価の一部として評価されるべきである。そして、この規則の要件を適用できることは、関連する欧州連合整合化立法の下における適合性評価の個々の論理、手法または一般構造に対して影響を与えてはならない。

It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation based on the New Legislative Framework, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already provided for in that law. The applicability of the requirements of

this Regulation should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant Union harmonisation legislation.

- (125) 高リスク AI システムの複雑性及びそれと関係するリスクに鑑み、指定組織が関与する高リスク AI システムに関する適合性評価手続という適切な制度、すなわち、いわゆる第三者適合性評価を発展させることが重要である。ただし、製品の安全性の分野における職業的な市場化前認証者の現在の経験及び関係するリスクの性質の相違に鑑み、製品と関連する第三者適合性評価以外の高リスク AI システムの第三者適合性評価の適用範囲を、少なくともこの規則の適用の最初の段階に制限することが適切である。それゆえ、そのようなシステムの適合性評価は、生体要素を利用することを意図する AI システムを唯一の例外とし、原則として、当該システムの提供者自身の責任の下においてその提供者によって実施されるべきである。

Given the complexity of high-risk AI systems and the risks that are associated with them, it is important to develop an adequate conformity assessment procedure for high-risk AI systems involving notified bodies, so-called third party conformity assessment. However, given the current experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for biometrics.

- (126) そのように要求される場合において第三者適合性評価を遂行するため、とりわけ、独立性、能力、利益相反の不存在及び適切なサイバーセキュリティの各要件に関し、諸要件のセットをその組織が遵守していることを条件として、この規則の下において、職務権限のある国内機関から、指定組織が通知されるべきである。それらの組織の通知は、職務権限のある国内機関から、欧州委員会及び他の構成国に対し、決定 No 768/2008/EC の別紙 I の R23 条により欧州委員会によって開発及び運営管理される電子的な通知ツールを用いて送付されるべきである。

In order to carry out third-party conformity assessments when so required, notified bodies should be notified under this Regulation by the national competent authorities, provided that they comply with a set of requirements, in particular on independence, competence, absence of conflicts of interests and suitable cybersecurity requirements. Notification of those bodies should be sent by national competent authorities to the Commission and the other Member States by means of the electronic notification tool developed and managed by the Commission pursuant to Article R23 of Annex I to Decision No 768/2008/EC.

- (127) 貿易の技術的障害に関する世界貿易機関の協定の下における欧州連合の確約に沿って、その組織が拠点をもつ領土に拘わらず、第三国の法律の下で設立された当該適合性評価組織がこの規則の適用可能な要件に適合すること、及び、その範囲において欧州連合が協定を締結したことを条件として、職務権限のある適合性評価組織によって作成された適合性評価結果の相互承認を促進することが適切である。その過程において、欧州委員会は、その目的のための可能な国際的法律文書を積極的に開拓すべきであり、かつ、とりわけ、第三国との間の相互承認協定の締結を求めるべき

である。

In line with Union commitments under the World Trade Organization Agreement on Technical Barriers to Trade, it is adequate to facilitate the mutual recognition of conformity assessment results produced by competent conformity assessment bodies, independent of the territory in which they are established, provided that those conformity assessment bodies established under the law of a third country meet the applicable requirements of this Regulation and the Union has concluded an agreement to that extent. In this context, the Commission should actively explore possible international instruments for that purpose and in particular pursue the conclusion of mutual recognition agreements with third countries.

- (128) 欧州連合整合化立法によって規律される製品に関する実質的な修正という共通に確立された概念に沿って、高リスク AI システムがこの規則を遵守することに影響を与え得る変更(例: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)が生じたときは常に、または、そのシステムの所期の目的を変更する場合においては、当該 AI システムが、新たな適合性評価が実施されるべき新たな AI システムであると判断されるべきであることが適切である。ただし、市場に置かれた後またはサービスに供された後においても「学習」を継続する AI システム、すなわち、機能がどのように実行されるかを自動的に調整する AI システムのアルゴリズム及びその性能に生ずる変更は、当該変更が提供者によって事前に決定されており、かつ、適合性評価の際に評価されていることを条件として、実質的な修正を組成してはならない。

In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that whenever a change occurs which may affect the compliance of a high-risk AI system with this Regulation (e.g. change of operating system or software architecture), or when the intended purpose of the system changes, that AI system should be considered to be a new AI system which should undergo a new conformity assessment. However, changes occurring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service, namely automatically adapting how functions are carried out, should not constitute a substantial modification, provided that those changes have been pre-determined by the provider and assessed at the moment of the conformity assessment.

- (129) 高リスク AI システムは、当該 AI システムが域内市場内を支障なく移動できるようにするため、当該 AI システムがこの規則に適合していることを表示するための CE マークを付すべきである。製品の中に組み込まれる高リスク AI システムに関しては、物理的な CE マークが付されるべきであり、かつ、デジタルの CE マークによって補完され得る。デジタルにのみ提供される高リスク AI システムに関しては、デジタルの CE マークが用いられるべきである。構成国は、この規則の中で定められた要件を遵守しており、かつ、CE マークを付している高リスク AI システムを市場に置きまたはサービスに供することを妨げる正当化されない 障碍をつくり出してはならない。

High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. For high-risk AI systems embedded in a product, a physical CE marking should be affixed, and may be complemented by a digital CE marking. For high-risk AI systems only provided digitally, a

digital CE marking should be used. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

- (130) 一定の条件の下において、革新的な技術の迅速な可用性は、個人の健康及び安全、環境の保護と気候変動及び社会全体にとって重要であり得る。そして、公共の保安または自然人の生命と健康の保護、環境の保護及び鍵となる産業資産とインフラ資産の保護という例外的な理由に基づき、適合性評価を受けていない AI システムを市場に置くことまたはサービスに供することを市場監視当局が認め得ることが適切である。この規則の中で定められた適正に正当化される状況下において、法執行機関または市民保護機関は、その利用中または利用後に不適切な遅滞なくそのような許可が求めら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、特定の高リスク AI システムをサービスに供することができる。

Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons, the protection of the environment and climate change and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons, environmental protection and the protection of key industrial and infrastructural assets, market surveillance authorities could authorise the placing on the market or the putting into service of AI systems which have not undergone a conformity assessment. In duly justified situations, as provided for in this Regulation, law enforcement authorities or civil protection authorities may put a specific high-risk AI system into service without the authorisation of the market surveillance authority, provided that such authorisation is requested during or after the use without undue delay.

- (131) AI の分野における欧州委員会と構成国の作業を容易にするため、及び、公衆に向けた透明性を増加させるため、関連する現行の欧州連合整合化立法の適用範囲内にある製品と関係のあるシステム以外の高リスク AI システムの提供者、及び、特例を基礎として、この規則の別紙中の高リスク利用の場合に列挙されている AI システムが高リスクではないと判断する提供者は、その提供者自身及びその提供者の AI システムに関する情報を、欧州委員会によって設置及び運営管理される EU データベースに登録することが要求されるべきである。この規則の別紙中の高リスク利用の場合に列挙されている AI システムを利用する前に、行政機関、行政部局または行政組織である高リスク AI システムの設置者は、その設置者自身をそのようなデータベースに登録し、かつ、その機関等が利用を予定するシステムを選択すべきである。それ以外の設置者は、任意でそのようにする資格を与えられるべきである。EU データベースのこのセクションは無料で公表されるべきであり、その情報は、容易にナビゲート可能であり、理解でき、かつ、機械読取可能であるべきである。EU データベースは、例えば、キーワードによる場合を含め、高リスク AI システムの登録に基づき及びこの規則の別紙の中で定められる高リスク AI システムの利用の場合に関し、それに対応する高リスク AI システムの適格な情報を一般公衆が見つかることができる検索機能を提供することによって、ユーザフレンドリでもあるべきである。高リスク AI システムの実質的な修正も EU データベースに登録されるべきである。法執行、移民、難民及び出入国管理の分野における高リスク AI システムに関しては、その登録義務は、EU データベースの安全で非公開のセクションの中で履行されるべきである。安全で非公開のセクションへのアクセスは、欧州委員会に厳格に制限され、また、同データベースの市場監視当局の国内

セクションに関しては市場監視当局に厳格に制限されるべきである。不可欠インフラの分野における高リスク AI システムは、国内レベルにおいてのみ登録されるべきである。欧州委員会は、規則(EU) 2018/1725 に従い、EU データベースの管理者であるべきである。EU データベースの全面的な稼働を確保するため、設置の際、そのデータベースの設定の手続は、欧州委員会による機能仕様書及び独立の監査報告書の作成を含めるべきである。欧州委員会は、EU データベースのデータ管理者としてのその職務を実施する際、サイバーセキュリティ上のリスクを考慮に入れるべきである。公衆による同データベースの可用性及び利用を最大化させるため、EU データベースは、同データベースによって利用できるようにされる情報を含め、指令(EU) 2019/882 の下にある要件を遵守すべきである。

In order to facilitate the work of the Commission and the Member States in the AI field as well as to increase the transparency towards the public, providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, as well as providers who consider that an AI system listed in the high-risk use cases in an annex to this Regulation is not high-risk on the basis of a derogation, should be required to register themselves and information about their AI system in an EU database, to be established and managed by the Commission. Before using an AI system listed in the high-risk use cases in an annex to this Regulation, deployers of high-risk AI systems that are public authorities, agencies or bodies, should register themselves in such database and select the system that they envisage to use. Other deployers should be entitled to do so voluntarily. This section of the EU database should be publicly accessible, free of charge, the information should be easily navigable, understandable and machine-readable. The EU database should also be user-friendly, for example by providing search functionalities, including through keywords, allowing the general public to find relevant information to be submitted upon the registration of high-risk AI systems and on the use case of high-risk AI systems, set out in an annex to this Regulation, to which the high-risk AI systems correspond. Any substantial modification of high-risk AI systems should also be registered in the EU database. For high-risk AI systems in the area of law enforcement, migration, asylum and border control management, the registration obligations should be fulfilled in a secure non-public section of the EU database. Access to the secure non-public section should be strictly limited to the Commission as well as to market surveillance authorities with regard to their national section of that database. High-risk AI systems in the area of critical infrastructure should only be registered at national level. The Commission should be the controller of the EU database, in accordance with Regulation (EU) 2018/1725. In order to ensure the full functionality of the EU database, when deployed, the procedure for setting the database should include the development of functional specifications by the Commission and an independent audit report. The Commission should take into account cybersecurity risks when carrying out its tasks as data controller on the EU database. In order to maximise the availability and use of the EU database by the public, the EU database, including the information made available through it, should comply with requirements under the Directive (EU) 2019/882.

- (132) 自然人とやりとりすることまたはコンテンツを生成することを意図する一定の AI システムは、そのシステムが高リスクとして分類されるか否かを問わず、なりすままたは偽装という個別のリスクを呈することがあり得る。それゆえ、一定の状況の下においては、それらのシステムの利用は、高リスク AI システムの要件及び義務を妨げることなく、かつ、法執行の特別の必要性を考慮に入れるための目的を絞った適用除外に服して、個別的な透明性義務に服すべきである。とりわけ、自然人は、合理的に十分な事前の説明を受け、状況及び利用過程を考慮に入れた上で観察及び用心する自然人という視点

から見てそのことが明白ではない限り、その者が AI システムとやりとりしていることの通知を受けるべきである。その義務を実装する際、それらの自然人の年齢または障害のゆえに脆弱なグループに属する自然人の特性は、その AI システムがそれらのグループなどとやりとりすることを意図している範囲内において、考慮に入れられるべきである。それに加えて、自然人は、その自然人の生体要素データを処理することによって、個人の感情もしくは意図を特定もしくは推論でき、または、個人を特別の類型に振り分けることができる AI システムにそれらの自然人が直面しているときは、その通知を受けるべきである。そのような特別の類型は、性、年齢、髪の色、眼の色、刺青、個人的な特徴、民族的な出自、個人の指向及び興味のような側面と関係し得る。そのような情報提供及び通知は、障害をもつ者にとってアクセス可能な方式で提供されるべきである。

Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems and subject to targeted exceptions to take into account the special need of law enforcement. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect taking into account the circumstances and the context of use. When implementing that obligation, the characteristics of natural persons belonging to vulnerable groups due to their age or disability should be taken into account to the extent the AI system is intended to interact with those groups as well. Moreover, natural persons should be notified when they are exposed to AI systems that, by processing their biometric data, can identify or infer the emotions or intentions of those persons or assign them to specific categories. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, personal traits, ethnic origin, personal preferences and interests. Such information and notifications should be provided in accessible formats for persons with disabilities.

- (133) ある種類の AI システムは、人間が生成したコンテンツ及び真正なコンテンツと区別することが人間にとって次第に困難になっている莫大な量の合成コンテンツを生成できる。それらのシステムが広範な可用性をもつこととその実現能力が増大していることは、情報のエコシステムの完全性と信頼に対して重大な影響をもち、偽情報と大規模な情報操作、詐偽、なりすまし及び消費者に対する欺瞞行為という新たなリスクを生じさせている。それらの影響、技術の速いペース及び情報の出所を追跡するための新たな手法と技法の必要性に照らし、それらのシステムの提供者に対し、その出力が AI システムによって生成または操作されたものであり、人間によるものではないことの機械読取可能なフォーマットによるマーキングと検出を実現可能とする技術上のソリューションを組み込むことを要求するのが適切である。そのような技法及び手法は、電子透かし、メタデータ識別子、コンテンツの出所と真正性を証明するための暗号化手法、履歴管理手法、電子指紋またはそれ以外の技法のような、利用可能な技法及びそのような技法の組合せをしかるべく考慮に入れた上で、それが技術的に利用可能な限り、十分な信頼性があり、相互運用性があり、実効性があり、かつ、堅牢であるべきである。この義務を実装する際、提供者は、一般的に承認されている最新技術を反映させて、異なるタイプのコンテンツの特性と制限、及び、その分野における関連技術の発展及び市場の発展も考慮に入れるべきである。そのような技法及び手法は、一般目的 AI モデルが生成するコンテンツを含め、AI システムのレベルでまたは AI モデルのレベルで実装され得るのであり、それによって、その AI システムの

下流の提供者によるこの義務の履行を容易にし得る。比例性を維持するため、このマーキングの義務が、標準的な編集作業のための基本的に補助的な機能を遂行する AI システム、または、設置者から提供された入力データもしくはそのセマンティクスを大きく改変しない AI システムを包摂してはならないということを用意するのが適切である。

A variety of AI systems can generate large quantities of synthetic content that becomes increasingly hard for humans to distinguish from human-generated and authentic content. The wide availability and increasing capabilities of those systems have a significant impact on the integrity and trust in the information ecosystem, raising new risks of misinformation and manipulation at scale, fraud, impersonation and consumer deception. In light of those impacts, the fast technological pace and the need for new methods and techniques to trace origin of information, it is appropriate to require providers of those systems to embed technical solutions that enable marking in a machine readable format and detection that the output has been generated or manipulated by an AI system and not a human. Such techniques and methods should be sufficiently reliable, interoperable, effective and robust as far as this is technically feasible, taking into account available techniques or a combination of such techniques, such as watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, **fingerprints** or other techniques, **as may be appropriate**. When implementing this obligation, providers should also take into account the specificities and **the** limitations of the different types of content and the relevant technological and market developments in the field, as reflected in the generally acknowledged state of the art. Such techniques and methods can be implemented at the level of the AI system or at the level of the AI model, including general-purpose AI models generating content, thereby facilitating fulfilment of this obligation by the downstream provider of the AI system. To remain proportionate, it is appropriate to envisage that this marking obligation should not cover AI systems performing primarily an assistive function for standard editing or AI systems not substantially altering the input data provided by the deployer or the semantics thereof.

- (134) AI システムの提供者によって稼働させられる技術上のソリューションとは別に、実在の者、対象物、場所、法主体または出来事と酷似しており、かつ、人に対してそれが真正なものもしくは真実のものであるかのように偽って表出されるような画像、音響または映像のコンテンツを生成または操作すること(「ディープフェイク」)のために AI システムを利用する設置者もまた、AI の出力をしかるべくラベリングし、それが人工的な出自のものであることを開示することによって、そのコンテンツが人工的に生成または操作されたものであることを明確かつ区別可能な状態で開示すべきである。とりわけ、そのコンテンツが、第三者の権利及び自由の適切な安全確保に服し、明らかに創造的、風刺的、芸術的またはフィクションもしくはアナロジーの作品またはプログラムの一部である場合において、この透明性義務を遵守することは、その AI システムまたはそのシステムの出力を利用することが憲章の中で保障されている表現の自由の権利並びに芸術及び科学の自由の権利を侵害することを示すものとして解釈されてはならない。それらの場合において、この規則に定めるディープフェイクに関する透明性義務は、その作品の有用性と品質を維持しつつ、その作品の通常の使用及び利用を含め、その作品の展示または鑑賞を妨げない適切な態様で、そのような生成または操作されたコンテンツが存在することの開示に限定される。加えて、当該 AI 生成コンテンツが、人間による見直しまたは編集管理のプロセスを実施したものであり、かつ、そのコンテンツの公表に関して自然人または法人が編集者の責任を負う場合を除き、公共の利益にかかわる事柄を公衆に対して情報提供することを目的として当

該文が公表される範囲内において、AI が生成または操作した文との関係においても類似の開示義務を予定することが適切である。

Further to the technical solutions employed by the providers of the AI system, deployers who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful (deep fakes), should also clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the AI output accordingly and disclosing its artificial origin. Compliance with this transparency obligation should not be interpreted as indicating that the use of the AI system or its output impedes the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter, in particular where the content is part of an evidently creative, satirical, artistic, fictional or analogous work or programme, subject to appropriate safeguards for the rights and freedoms of third parties. In those cases, the transparency obligation for deep fakes set out in this Regulation is limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work, including its normal exploitation and use, while maintaining the utility and quality of the work. In addition, it is also appropriate to envisage a similar disclosure obligation in relation to AI-generated or manipulated text to the extent it is published with the purpose of informing the public on matters of public interest unless the AI-generated content has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content.

- (135) 透明性義務の強制的な性質及び完全な適用可能性を妨げることなく、欧州委員会は、検知の仕組みにしかるべくアクセスできるようにすること、価値連鎖の流れに沿って他の関与者との間の協力を容易にすること、コンテンツを流通させること、または、AI 生成コンテンツであることを公衆が実効的に区別できるようにするためにそのコンテンツの真正性及び来歴を検査することに関する実務上の手立てを支援することを含め、人工的に生成または操作されたコンテンツの検出及びラベリングと関連する義務の実効的な実装を容易にするため、欧州連合レベルの実務準則を作成することも推進及び促進できる。

Without prejudice to the mandatory nature and full applicability of the transparency obligations, the Commission may also encourage and facilitate the drawing up of codes of practice at Union level to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content, including to support practical arrangements for making, as appropriate, the detection mechanisms accessible and facilitating cooperation with other actors along **the value chain**, disseminating content or checking its authenticity and provenance to enable the public to effectively distinguish AI-generated content.

- (136) 当該システムの出力が人工的に生成または操作されていることの検出及び開示を実現可能にするためのこの規則中にある一定の AI システムの提供者及び設置者に対して課される義務は、規則 (EU) 2022/2065 の実効的な実装を促進することと特に関連性がある。このことは、とりわけ、人工的に生成または操作されたコンテンツの流通から生じるかもしれないシステムリスク、とりわけ、偽情報による場合を含め、民主的な過程、市民の意見交換と選挙のプロセスに対する現実のまたは予測可能な負の影響というリスクを識別及び緩和すべき非常に大きなオンラインプラットフォームのプロバイダ

または非常に大きなオンライン検索エンジンのプロバイダの義務に関して適用される。この規則の下における AI システムによって生成されたコンテンツをラベルする要件は、規則(EU) 2022/2065 の第 16 条第 1 項により受領した違法なコンテンツに関する通報を処理すべきホスティングサービスプロバイダに関する同規則の第 16 条第 6 項の義務を妨げず、また、個々のコンテンツの違法性に関する評価及び判定に対して影響を与えてはならない。その評価は、当該コンテンツの違法性を規律する規定のみを参照して遂行されるべきである。

The obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular the risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation. The requirement to label content generated by AI systems under this Regulation is without prejudice to the obligation in Article 16(6) of Regulation (EU) 2022/2065 for providers of hosting services to process notices on illegal content received pursuant to Article 16(1) of that Regulation and should not influence the assessment and the decision on the illegality of the specific content. That assessment should be performed solely with reference to the rules governing the legality of the content.

- (137) この規則の適用を受ける AI システムに関する透明性義務の遵守は、この規則またはそれ以外の欧州連合法及び構成国法の下において AI システムまたはそのシステムの出力を利用することが適法であるということを示すものとして解釈されてはならず、かつ、欧州連合法または国内法に定める AI システムの設置者に課される他の透明性義務を妨げてはならない。

Compliance with the transparency obligations for the AI systems covered by this Regulation should not be interpreted as indicating that the use of the AI system or its output is lawful under this Regulation or other Union and Member State law and should be without prejudice to other transparency obligations for deployers of AI systems laid down in Union or national law.

- (138) AI は、責任ある技術革新及び適切な安全確保措置とリスク緩和措置の統合を確保しつつ、法制上の監視及び実験のための安全かつ管理された空間を必要とする諸技術の急速に発展しているファミリーである。技術革新を促進する法的枠組みが将来耐性と混乱に抗する回復力をもつことを確保するため、構成国は、その構成国の職務権限のある国内機関が、そのシステムが市場に置かれまたはサービスに供される前に、厳格な法制監視の下で革新的な AI システムの開発及び試験を促進するための少なくとも 1 つの AI 法制サンドボックスを国内レベルで構築することを確保すべきである。構成国は、参加構成国に対して均等なレベルの国内適用をその参加が提供している範囲内において、既存の法制サンドボックスに参加することにより、または、1 もしくは複数の構成国の職務権限のある機関と共同してサンドボックスを開設することによってもこの義務を満たし得る。AI 法制サンドボックスは、物理的な形態、デジタルの形態またはハイブリッドの形態で設けられ得るのであり、また、物理的な製品とデジタルの製品に対応できる。開設当局は、その AI 法制サンドボックスが、資金及び

人的資源を含め、その稼働のための十分な資源をもつことも確保すべきである。

AI is a rapidly developing family of technologies that requires regulatory oversight and a safe and controlled space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that promotes innovation, is future-proof and resilient to disruption, Member States should ensure that their national competent authorities establish at least one AI regulatory sandbox at national level to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service. Member States could also fulfil this obligation through participating in already existing regulatory sandboxes or establishing jointly a sandbox with one or more Member States' competent authorities, insofar as this participation provides equivalent level of national coverage for the participating Member States. AI regulatory sandboxes could be established in physical, digital or hybrid form and may accommodate physical as well as digital products. Establishing authorities should also ensure that the AI regulatory sandboxes have the adequate resources for their functioning, including financial and human resources.

- (139) AI 法制サンドボックスの目的は、革新的な AI システムが、この規則及び欧州連合と構成国の他の関連立法を遵守することを確保するという観点から、開発と市場化前の段階における管理された実験及び試験の環境を構築することにより、AI の技術革新を育成することにあるべきである。それに加えて、AI 法制サンドボックスは、革新的開発者のための法的確実性を拡大し、また、AI 利用の機会、リスクの発生及び影響に関する職務権限のある機関の監視と理解を拡大すること、法的枠組みの将来の調整という観点も含め、当局と企業にとっての法制の学習を容易にすること、AI 法制サンドボックスに関与する当局との間の協力とベストプラクティスの共有を支援すること、そして、スタートアップを含め、SMEs に関する障壁を除去することによる場合を含めて、市場へのアクセスを加速させることも狙いとしている。AI 法制サンドボックスは、欧州連合全域にわたって広範囲に利用できるべきであり、また、スタートアップを含め、SMEs に対して AI 法制サンドボックスへのアクセシビリティが与えられるべきであるということに特別の注意が払われるべきである。AI 法制サンドボックスへの参加は、技術革新のため、欧州連合内において AI を実験するため、そして、証拠ベースの法制学習に貢献するため、提供者及び見込提供者に対して法的不確実性を生じさせる問題に焦点を当てるべきである。それゆえ、AI 法制サンドボックス内における AI システムの監視は、そのシステムが市場に置かれまたはサービスに供される前におけるそのシステムの開発、訓練、試験及び検証並びに新たな適合性評価手続を必要とするかもしれない実質的な修正の概念と発生を含めるべきである。そのような AI システムの開発及び試験の間に発見された重大なリスクは、適切な緩和を帰結すべきであり、また、その失敗の場合には、開発と試験のプロセスの停止を帰結すべきである。それが適切なときは、AI 法制サンドボックスを構築する職務権限のある国内機関は、基本的な権利の保護を監督する機関を含め、他の適格のある機関と協力すべきであり、また、国内標準化組織及び欧州の標準化組織、指定組織、試験施設と実験施設、調査研究所と実験研究所、欧州デジタル技術革新ハブ並びに適格のある利害関係者及び市民社会団体のような、その AI エコシステム内にある他の関与者が関与することを許容し得る。欧州連合全域にわたる統一的な実装と規模の経済を確保するため、AI 法制サンドボックスの実装に関する共通規定及びサンドボックスの監督に関与する適格のある機関の間の協力の枠組みを設けることが適切である。この規則の下において開設される AI 法制サンドボックスは、この規則以外の法律の遵守を確保することを狙いとする別のサンドボックスの開設を認める別の法律を

妨げてはならない。それが適切なときは、それらの別の法制サンドボックスを担当する適格な職務権限のある機関は、AI システムがこの規則を遵守することを確保する目的のためにも当該別の法制サンドボックスを利用することの受益を検討すべきである。職務権限のある国内機関と AI 法制サンドボックスへの参加者との間の合意に基づき、実世界条件下の試験もまた、AI 法制サンドボックスの枠組みの中で運用され及び監督され得る。

The objectives of the AI regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and national law. Moreover, the AI regulatory sandboxes should aim to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, to facilitate regulatory learning for authorities and undertakings, including with a view to future adaptations of the legal framework, to support cooperation and the sharing of best practices with the authorities involved in the AI regulatory sandbox, and to accelerate access to markets, including by removing barriers for SMEs, including start-ups. AI regulatory sandboxes should be widely available throughout the Union, and particular attention should be given to their accessibility for SMEs, including start-ups. The participation in the AI regulatory sandbox should focus on issues that raise legal uncertainty for providers and prospective providers to innovate, experiment with AI in the Union and contribute to evidence-based regulatory learning. The supervision of the AI systems in the AI regulatory sandbox should therefore cover their development, training, testing and validation before the systems are placed on the market or put into service, as well as the notion and occurrence of substantial modification that may require a new conformity assessment procedure. Any significant risks identified during the development and testing of such AI systems should result in adequate mitigation and, failing that, in the suspension of the development and testing process. Where appropriate, national competent authorities establishing AI regulatory sandboxes should cooperate with other relevant authorities, including those supervising the protection of fundamental rights, and could allow for the involvement of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs, European Digital Innovation Hubs and relevant stakeholder and civil society organisations. To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the AI regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. AI regulatory sandboxes established under this Regulation should be without prejudice to other law allowing for the establishment of other sandboxes aiming to ensure compliance with law other than this Regulation. Where appropriate, relevant competent authorities in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may also be operated and supervised in the framework of the AI regulatory sandbox.

- (140) この規則は、規則(EU) 2016/679 の第 6 条第 4 項及び第 9 条第 2 項(g)並びに規則(EU) 2018/1725 の第 5 条、第 6 条及び第 10 条に沿って、かつ、指令(EU) 2016/680 の第 4 条第 2 項及び第 10 条を妨げることなく、AI 法制サンドボックス内の提供者及び見込提供者に対し、個別の条件の下にある場合に限り、当該 AI 法制サンドボックス内における公共の利益における一定の AI システムの開発のた

めに、別の目的のために収集された個人データを利用するための適法性の根拠を提供すべきである。規則(EU) 2016/679, 規則(EU) 2018/1725 及び指令(EU) 2016/680 の下にあるデータ管理者の他の全ての義務及びデータ主体の全ての権利は、適用可能なままである。とりわけ、この規則は、規則(EU) 2016/679 の第 22 条第 2 項(b)及び規則(EU) 2018/1725 の第 24 条第 2 項(b)の意味における適法性の根拠を提供してはならない。AI 法制サンドボックス内の提供者及び見込提供者は、サンドボックス内の開発、試験及び実験の間に生じ得る安全、健康及び基本的な権利を妨げる識別された重大なリスクを適切に緩和するため、職務権限のある機関の指針に従うこと、及び、迅速かつ誠実に行動することによる場合を含め、適切な安全確保を確保し、かつ、職務権限のある機関と協力すべきである。

This Regulation should provide the legal basis for the providers and prospective providers in the AI regulatory sandbox to use personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, only under specified conditions, in accordance with Article 6(4) and Article 9(2), point (g), of Regulation (EU) 2016/679, and Articles 5, 6 and 10 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) and Article 10 of Directive (EU) 2016/680. All other obligations of data controllers and rights of data subjects under Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis in the meaning of Article 22(2), point (b) of Regulation (EU) 2016/679 and Article 24(2), point (b) of Regulation (EU) 2018/1725. Providers and prospective providers in the AI regulatory sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to adequately mitigate any identified significant risks to safety, health, and fundamental rights that may arise during the development, testing and experimentation in that sandbox.

- (141) この規則の別紙の中に列挙される高リスク AI システムの開発のプロセス及び市場に置くことを加速させるため、そのようなシステムの提供者及び見込提供者が、AI 法制サンドボックスに参加することなく、実世界条件下でそれらのシステムを試験するための特別な制度からも受益できることが重要である。ただし、そのような場合においては、そのような試験の個人に対するあり得る結果を考慮に入れた上で、提供者及び見込提供者に関し、適切かつ十分な保証及び条件がこの規則によって導入されることが確保されるべきである。そのような保証は、就中、事前の説明を受けた上での同意を要求することが当該 AI システムの試験を妨げるような場合における法執行の適用除外を伴うが、実世界条件下の試験に参加するための自然人の事前の説明を受けた上での同意を必要とすることを含めるべきである。この規則の下においてそのような試験に参加するための主体の同意は、関連データ保護法に基づく当該データ主体の個人データの処理に関するデータ主体の同意とは別のものであり、かつ、その同意を妨げない。そのリスクをミニマム化すること、職務権限のある機関による監督を実現可能にすること、及び、それゆえに、見込提供者に対し、職務権限のある市場監視当局に対して提出される実世界試験計画書をもつこと、幾つかの限定的な適用除外に服して EU データベースの専用セクションに当該試験を登録すること、試験が実施され得る期間の制限を設定することを要求すること、そして、一定の脆弱なグループに属する個人のための付加的な安全確保及び見込提供者と設置者の責任と役割を定義する書面による合意並びにその実世界試験に関与する職務権限のある担当者による実効的な監督を要求することも重要である。更に、AI システムの予測、推奨または判定が実効的に覆され及び無視され得ること、そして、欧州連合のデータ保護法の下にあるデータ主体

としての当該の者の権利を妨げることなく、その主体が、当該試験に参加するためのその主体の同意を撤回したときは、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の付加的な安全確保を予定することが適切である。非個人データに関しては、欧州議会及び理事会の規則(EU) 2022/868⁴²及び規則(EU) 2023/2854⁴³のような欧州連合法に従って適切な安全確保が設けられているが、データの移転に関しては、欧州連合法の下にある適切かつ適用可能な安全確保が実装されている場合に限り、特にデータ保護に関する欧州連合法の下にある個人データの移転のための根拠に従い、実世界条件下の試験の目的のために収集され及び処理されるデータが欧州連合の外にある第三国に対して移転されるべきことを予定することも適切である。

In order to accelerate the process of development and the placing on the market of the high-risk AI systems listed in an annex to this Regulation, it is important that providers or prospective providers of such systems may also benefit from a specific regime for testing those systems in real world conditions, without participating in an AI regulatory sandbox. However, in such cases, taking into account the possible consequences of such testing on individuals, it should be ensured that appropriate and sufficient guarantees and conditions are introduced by this Regulation for providers or prospective providers. Such guarantees should include, inter alia, requesting informed consent of natural persons to participate in testing in real world conditions, with the exception of law enforcement where the seeking of informed consent would prevent the AI system from being tested. Consent of subjects to participate in such testing under this Regulation is distinct from, and without prejudice to, consent of data subjects for the processing of their personal data under the relevant data protection law. It is also important to minimise the risks and enable oversight by competent authorities and therefore require prospective providers to have a real-world testing plan submitted to competent market surveillance authority, register the testing in dedicated sections in the EU database subject to some limited exceptions, set limitations on the period for which the testing can be done and require additional safeguards for persons belonging to certain vulnerable groups, as well as a written agreement defining the roles and responsibilities of prospective providers and deployers and effective oversight by competent personnel involved in the real world testing. Furthermore, it is appropriate to envisage additional safeguards to ensure that the predictions, recommendations or decisions of the AI system can be effectively reversed and disregarded and that personal data is protected and is deleted when the subjects have withdrawn their consent to participate in the testing without prejudice to their rights as data subjects under the Union data protection law. As regards transfer of data, it is also appropriate to envisage that data collected and processed for the purpose of testing in real-world conditions should be transferred to third countries only where appropriate and applicable safeguards under Union law are implemented, in particular in accordance with bases for transfer of personal data under

⁴² 欧州のデータ統治に関する及び規則(EU) 2018/1724を改正する欧州議会及び理事会の 2022 年 5 月 30 日の規則(EU)2022/868(データ統治法)(OJ L 152, 3.6.2022, p. 1).

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1).

⁴³ データへの公正なアクセス及びその利用に関する整合化された規定に関する、並びに、規則(EU) 2017/2394 及び指令 (EU) 2020/1828 を改正する欧州議会及び理事会の 2023 年 12 月 13 日の規則(EU) 2023/2854(データ法)(OJ L, 2023/2854).

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

Union law on data protection, while for non-personal data appropriate safeguards are put in place in accordance with Union law, such as Regulations (EU) 2022/868⁽⁴²⁾ and (EU) 2023/2854⁽⁴³⁾ of the European Parliament and of the Council.

- (142) AI が社会上及び環境上の有益な成果を導くことを確保するため、構成国は、障害をもつ者のアクセシビリティを向上させるための AI を基礎とするソリューションのような、社会上及び環境上の有益な成果を支える AI ソリューションの調査研究及び開発を支援及び促進すること、社会経済的な不平等と取り組むこと、または、公的資金及び欧州連合の基金を含め、十分な資源を割当てることによって、また、それが適切なときは、かつ、資格と選定基準が満たされていることを条件として、とりわけ、そのような諸目的を求めるプロジェクトを考慮することによって、環境上の目標に適合することが推奨される。そのようなプロジェクトは、AI 開発者、不平等及び不差別、アクセシビリティ、消費者の権利、環境の権利及びデジタル権利に関する専門家並びに学术界の間における学際的な協力の諸原則を基礎とすべきである。

To ensure that AI leads to socially and environmentally beneficial outcomes, Member States are encouraged to support and promote research and development of AI solutions in support of socially and environmentally beneficial outcomes, such as AI-based solutions to increase accessibility for persons with disabilities, tackle socio-economic inequalities, or meet environmental targets, by allocating sufficient resources, including public and Union funding, and, where appropriate and provided that the eligibility and selection criteria are fulfilled, considering in particular projects which pursue such objectives. Such projects should be based on the principle of interdisciplinary cooperation between AI developers, experts on **inequality and non-discrimination**, accessibility, consumer, environmental, and digital rights, as well as academics.

- (143) 技術革新を促進及び保護するため、スタートアップを含め、AI システムの提供者または設置者である SMEs の利益が特に考慮に入れられることが重要である。その目的のために、構成国は、認識向上及び情報伝達に関するものを含め、それらの運営者に目的を絞った取り組みを發展させるべきである。構成国は、スタートアップを含め、欧州連合内における登録された事務所または支社をもつ SMEs に対し、その SMEs が資格条件と選定基準を満たしていることを条件として、かつ、同じ条件及び基準を満たされている限り SMEs 以外の提供者及び見込提供者が AI 法制サンドボックスにアクセスすることを妨げることなく、そのサンドボックスへの優先的なアクセスを提供すべきである。構成国は、この規則の実装に関する指針を提供すること及び質問に対して回答することによって開発段階全体を通じて SMEs を支援するため、スタートアップを含め SMEs、設置者、それら以外の革新的開発者、及び、しかるべく、地方行政機関との間の通信のために、既存の経路を活用すべきであり、または、それが適切なときは、新たな専用の経路を設けるべきである。それが適切なときは、波及効果をつくり出すため、及び、スタートアップを含め SMEs と設置者に対するそれらの経路の指針における均質性を確保するため、それらの経路は、共働すべきである。加えて、構成国は、標準化策定過程への SMEs 及びそれ以外の適格な利害関係者の参加を容易にすべきである。更に、指定組織が適合性評価の手数料を定める際、スタートアップを含め SMEs である提供者の個別の利益及び需要が考慮に入れられるべきである。欧州委員会は、透明性のある意見聴取を通じて、スタートアップを含め SMEs にかかる認証及び遵守の費用を定期的に評価すべきであり、また、そのような費用を低くする

ため、構成国と共働すべきである。例えば、作成義務のある文書の翻訳及び当局との間の通信と関連する費用は、提供者及びそれ以外の運用者にとって、特に小規模な運用者にとって、大きな費用を組成し得る。構成国は、それが可能であれば、関連提供者の文書化のため及び運用者との間の通信のために当該構成国によって定められ及び承認される言語中の 1 つが、最大多数の国境を越える設置者によって広範に理解される言語であることを確保すべきである。スタートアップを含め SMEs の個別の需要に対処するため、欧州委員会は、委員会の要請に応じて、この規則の適用のある分野のための標準化された雛型を提供すべきである。それに加えて、欧州委員会は、この規則と関連する利用しやすい情報を全ての提供者及び設置者に対して提供する単一情報提供プラットフォームを提供することにより、この規則から生ずる義務に関する認識向上のための適切な情報伝達キャンペーンを準備することにより、そして、AI システムと関連する公共調達手続におけるベストプラクティスの収斂を評価及び促進することにより、構成国の努力を補完すべきである。委員会勧告 2003/361/EC⁴⁴の別紙の意味における小規模に最近まで分類されていた中規模企業は、それらの新たに定義された中規模企業が、時として、この規則の適切な理解と遵守を確保するための法情報源と訓練を欠いているので、それらの支援措置へのアクセスをもつべきである。

In order to promote and protect innovation, it is important that the interests of SMEs, including start-ups, that are providers or deployers of AI systems are taken into particular account. To that end, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Member States should provide SMEs, including start-ups, that have a registered office or a branch in the Union, with priority access to the AI regulatory sandboxes provided that they fulfil the **conditions** and selection criteria and without precluding other providers and prospective providers to access the sandboxes provided the same conditions and criteria are fulfilled. Member States should utilise existing channels and where appropriate, establish new dedicated channels for communication with SMEs, including start-ups, deployers, other innovators and, as appropriate, local public authorities, to support SMEs throughout their development path by providing guidance and responding to queries about the implementation of this Regulation. Where appropriate, these channels should work together to create synergies and ensure homogeneity in their guidance to SMEs, including start-ups, and deployers. Additionally, Member States should facilitate the participation of SMEs and other relevant stakeholders in the standardisation development processes. Moreover, the specific interests and needs of providers that are SMEs, including start-ups, should be taken into account when notified bodies set conformity assessment fees. The Commission should regularly assess the certification and compliance costs for SMEs, including start-ups, through transparent consultations and should work with Member States to lower such costs. For example, translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, in particular those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border deployers. In order to address the specific needs of SMEs, including start-ups, the

⁴⁴ マイクロ企業、小企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告(OJ L 124, 20.5.2003, p. 36).

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Commission should provide standardised templates for the areas covered by this Regulation, upon request of the Board. Additionally, the Commission should complement Member States' efforts by providing a single information platform with easy-to-use information with regards to this Regulation for all providers and deployers, by organising appropriate communication campaigns to raise awareness about the obligations arising from this Regulation, and by evaluating and promoting the convergence of best practices in public procurement procedures in relation to AI systems. Medium-sized enterprises which until recently qualified as small enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC⁽⁴⁴⁾ should have access to those support measures, as those new medium-sized enterprises may sometimes lack the legal resources and training necessary to ensure proper understanding of, and compliance with, this Regulation.

- (144) 技術革新を促進及び保護するため、AI オンデマンドプラットフォーム、デジタル欧州計画、Horizon Europe のような、欧州連合レベルまたは国内レベルで欧州委員会及び構成国によって実装された欧州連合の適格な全ての基金計画及びプロジェクトは、しかるべく、この規則の目的の達成のために貢献すべきである。

In order to promote and protect innovation, the AI-on-demand platform, all relevant Union funding programmes and projects, such as Digital Europe Programme, Horizon Europe, implemented by the Commission and the Member States at Union or national level should, as appropriate, contribute to the achievement of the objectives of this Regulation.

- (145) 市場における知識及び専門知識の欠如から生じる実装のリスクをミニマム化するため、そして、この規則の下にある提供者、とりわけ、スタートアップを含め SMEs 及び指定組織の義務をそれらの者が遵守することを容易にするため、AI オンデマンドプラットフォーム、欧州デジタル技術革新ハブ、並びに、欧州委員会及び構成国によって欧州連合レベル及び国内レベルで設けられる試験施設及び実験施設は、この規則の実装に貢献すべきである。それらそれぞれの任務及び能力分野の範囲内において、AI オンデマンドプラットフォーム、欧州デジタル技術革新ハブ並びに試験施設及び実験施設は、提供者及び指定組織に対し、とりわけ、技術上及び科学上の支援を提供し得る。

In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers, in particular SMEs, including start-ups, and notified bodies with their obligations under this Regulation, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation facilities established by the Commission and the Member States at Union or national level should contribute to the implementation of this Regulation. Within their respective mission and fields of competence, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation **Facilities** are able to provide in particular technical and scientific support to providers and notified bodies.

- (146) それに加えて、非常に小規模な幾つかの運用者に照らし、かつ、技術革新の費用と関連する比例性を確保するため、マイクロ企業が最も費用のかかる義務の 1 つを履行できるようにすること、すなわち、保護のレベル及び高リスク AI システムに関する要件遵守の必要性を損なうことなく、それらの企業の行政上の負担と費用を削減し得るような簡素化された態様で、品質管理システムを設け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、マイクロ企業により、この簡素化された態様で満

たされるべき品質管理システムの諸要素を指定する指針を策定すべきである。

Moreover, in light of the very small size of some operators and in order to ensure proportionality regarding costs of innovation, it is appropriate to allow **microenterprises** to fulfil one of the most costly obligations, namely to establish a quality management system, in a simplified manner which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems. The Commission should develop guidelines to specify the elements of the quality management system to be fulfilled in this simplified manner by **microenterprises**.

- (147) 関連する欧州連合整合化立法により設立または承認され、かつ、その欧州連合整合化立法の適用のある製品または機器類の適合性評価の過程における職務を満たす組織、グループまたは研究施設に対し、欧州委員会が、それが可能な範囲内で、試験施設及び実験施設へのアクセスを容易にすることが適切である。特に、規則(EU) 2017/745 及び規則(EU) 2017/746 による医療機器の分野における専門家パネル、専門研究施設及び参考研究施設がそれに該当する。

It is appropriate that the Commission facilitates, to the extent possible, access to testing and experimentation facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is, in particular, the case as regards expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulations (EU) 2017/745 and (EU) 2017/746.

- (148) この規則は、国内レベルにおいてこの規則の適用を調整及び支援すること、並びに、欧州連合レベルで実現能力を構築すること及び AI の分野における利害関係者を統合することをいずれも可能とする統治枠組みを設けるべきである。この規則の実効的な実装及び執行は、欧州連合のレベルで調整し、かつ、中心的な専門知識を構築できるようにする統治枠組みを必要とする。AI 総局は、委員会決定⁴⁵により設けられ、AI の分野における欧州連合の専門知識と実現能力を開発すること及び AI に関する欧州連合法の実装に貢献することをその任務としてもつ。欧州連合の専門知識及び実現能力の開発を欧州連合レベルで支援すること、及び、デジタル単一市場の稼働を強化することという観点から、構成国は、AI 総局の職務を容易にすべきである。更に、構成国の代表によって構成される委員会、並びに、欧州連合レベル及び国内レベルにおいて、科学のコミュニティを統合するための科学パネル及びこの規則の実装への利害関係者の入力に寄与するための諮問フォーラムが設けられるべきである。欧州連合の専門知識及び実現能力の開発は、とりわけ、他の法律の欧州連合レベルの執行の過程において構築された構造の波及効果を通じて、そして、デジタル欧州計画の下にある EuroHPC 共同事業体及び AI 試験施設及び実験施設のような欧州連合レベルの関連する取組みとの波及効果を通じて、既存の資源及び専門知識を活用できるようにすることも含めるべきである。

⁴⁵ 欧州人工知能総局を設ける 2024 年 1 月 24 日の委員会決定 C(2024)390.
Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office C(2024)390.

This Regulation should establish a governance framework that both allows to coordinate and support the application of this Regulation at national level, as well as build capabilities at Union level and integrate stakeholders in the field of AI. The effective implementation and enforcement of this Regulation require a governance framework that allows to coordinate and build up central expertise at Union level. The AI Office was established by **Commission Decision**⁽⁴⁵⁾ and has as its mission to develop Union expertise and capabilities in the field of AI and to contribute to the implementation of Union law on AI. Member States should facilitate the tasks of the AI Office with a view to support the development of Union expertise and capabilities at Union level and to strengthen the functioning of the digital single market. Furthermore, a Board composed of representatives of the Member States, a scientific panel to integrate the scientific community and an advisory forum to contribute stakeholder input to the implementation of this Regulation, at Union and national level, should be established. The development of Union expertise and capabilities should also include making use of existing resources and expertise, in particular through synergies with structures built up in the context of the Union level enforcement of other law and synergies with related initiatives at Union level, such as the EuroHPC Joint Undertaking and the AI testing and experimentation facilities under the Digital Europe Programme.

- (149) この規則の円滑、実効的かつ整合性のとれた実装を容易にするため、委員会が設けられるべきである。委員会は、AI エコシステムの様々な利害関係を反映すべきであり、かつ、構成国の代表によって構成されるべきである。執行に関する事項、この規則の中で定められている要件と関連する技術仕様または既存の技術標準を含め、この規則の実装と関連する事項に関し、意見、勧告、助言を発することまたはそれと関連する指針に貢献すること、並びに、AI と関係する個別の問題に関し、欧州委員会及び構成国と構成国の職務権限のある国内機関に対して助言を提供することを含め、委員会は、多数の諮問の職務に関する職責を負うべきである。委員会における構成国の代表の任命において構成国に対してある程度の柔軟性を与えるため、そのような代表は、公的な法主体に属する者であり得る。その者は、国内レベルにおける調整を容易にするための適格な能力と権限をもち、かつ、委員会の職務の達成に貢献すべきである。委員会は、市場監視及び指定組織それぞれと関連する問題に関し、市場監視当局及び指定元当局の間における協力と意見交換のためのプラットフォームを提供する 2 つの常設サブグループを設けるべきである。市場監視に関する常設サブグループは、規則(EU) 2019/1020 の第 30 条の意味におけるこの規則のための行政協力グループ(ADCO)として行動すべきである。規則(EU) 2019/1020 の第 33 条に従い、欧州委員会は、とりわけ、市場監視当局の間の個別かつ緊急の調整を必要とするこの規則の側面を識別するという観点から市場の評価または研究を実施することによって、市場監視に関する常設サブグループの活動を支えるべきである。委員会は、個別の課題を審議する目的のために、常設または臨時の別のサブグループをしかるべく設け得る。委員会はまた、とりわけ、データ、デジタル製品及びデジタルサービスに関する適格な欧州連合法の下において能動的な組織等を含め、適格な欧州連合法の過程において能動的な適格な欧州連合の組織、専門家グループ及び専門家ネットワークとの間でしかるべく協力すべきである。

In order to facilitate a smooth, effective and harmonised implementation of this Regulation a Board should be established. The Board should reflect the various interests of the AI eco-system and be composed of representatives of the Member States. The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or contributing to guidance on matters related to the implementation of this Regulation, including on enforcement matters, technical specifications or existing standards regarding the requirements established

in this Regulation and providing advice to the Commission and the Member States and their national competent authorities on specific questions related to AI. In order to give some flexibility to Member States in the designation of their representatives in the Board, such representatives may be any persons belonging to public entities who should have the relevant competences and powers to facilitate coordination at national level and contribute to the achievement of the Board's tasks. The Board should establish two standing sub-groups to provide a platform for cooperation and **exchange** among market surveillance authorities and notifying authorities on issues related, **respectively, to market surveillance and notified bodies**. The standing subgroup for market surveillance should act as the administrative cooperation group (ADCO) for this Regulation within the meaning of Article 30 of Regulation (EU) 2019/1020. In accordance with Article 33 of that Regulation, the Commission should support the activities of the standing subgroup for market surveillance by undertaking market evaluations or studies, in particular with a view to identifying aspects of this Regulation requiring specific and urgent coordination among market surveillance authorities. The Board may establish other standing or temporary sub-groups as appropriate for the purpose of examining specific issues. The Board **should** also cooperate, as appropriate, with relevant Union bodies, experts groups and networks active in the context of relevant Union law, including in particular those active under relevant Union law on data, digital products and services.

- (150) この規則の実装及び適用における利害関係者の包摂を確保するという観点から、委員会及び欧州委員会に対して助言するため及び技術上の専門知識を提供するため、諮問フォーラムが設けられるべきである。商業的な利益と非商業的な利益との間の、及び、商業的な利益の種類の範囲内においては、SMEs 及びそれ以外の事業者に関し、利害関係者の多様かつバランスのとれた代表比率を確保するため、諮問フォーラムは、就中、産業界、スタートアップ、SMEs、学術界、ソーシャルパートナーを含め市民社会団体、並びに、基本的権利局、ENISA、欧州標準化委員会(CEN)、欧州電気技術標準化委員会(CENELEC)及び欧州電気通信標準機関(ETSI)によって構成されるべきである。

With a view to ensuring the involvement of stakeholders in the implementation and application of this Regulation, an advisory forum should be established to advise and provide technical expertise to the Board and the Commission. To ensure a varied and balanced stakeholder representation between commercial and non-commercial interest and, within the category of commercial interests, with regards to SMEs and other undertakings, the advisory forum should comprise inter alia industry, **start-ups**, SMEs, academia, **civil society**, including the social partners, as well as the Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI).

- (151) この規則の実装及び執行を支えるため、とりわけ、一般目的 AI モデルに関する AI 総局の監視活動を支えるため、独立の専門家の科学パネルが設けられるべきである。科学パネルを構成する独立の専門家は、AI の分野における最新の科学上または技術上の専門知識を基礎として選任されるべきであり、かつ、公平に、客観的に当該専門家の職務を遂行すべきであり、かつ、当該専門家の職務及び活動を実施する上で入手した情報及びデータの機密性を確保すべきである。この規則の実効的な執行のために必要となる国内の実現能力を強化できるようにするため、構成国は、構成国の執行活動のために、科学パネルを構成する専門家のプールからの支援を要請できるべきである。

To support the implementation and enforcement of this Regulation, in particular the monitoring activities of the AI Office as regards general-purpose AI models, a scientific panel of independent experts should be established. The independent experts constituting the scientific panel should be selected on the basis of up-to-date scientific or technical expertise in the field of AI and should perform their tasks with impartiality, objectivity and ensure the confidentiality of information and data obtained in carrying out their tasks and activities. To allow the reinforcement of national capacities necessary for the effective enforcement of this Regulation, Member States should be able to request support from the pool of experts constituting the scientific panel for their enforcement activities.

- (152) AI システムと関連する適切な執行を支えるため、及び、構成国の実現能力を強化するため、欧州連合の AI 試験支援機構が設けられ、かつ、構成国が採用できるようにすべきである。

In order to support adequate enforcement as regards AI systems and reinforce the capacities of the Member States, Union AI testing support structures should be established and made available to the Member States.

- (153) 構成国は、この規則の適用及び執行において、鍵となる役割をもつ。この点に関し、各構成国は、この規則の適用及び実装を監督する目的のための職務権限のある国内機関として、少なくとも 1 つの通知元当局及び少なくとも 1 つの市場監視当局を指定すべきである。構成国は、当該構成国の個別の国内組織上の特性及び需要に従い、この規則の意味における職務権限のある国内機関の職務を遂行するためのいずれかの公的法主体を指定することを決定できる。構成国の側における組織上の効率性を増加させるため、そして、構成国レベル及び欧州連合レベルにおける公衆とそれぞれの相手方との間の単一連絡部局を設置するため、各構成国は、単一連絡部局として行動する市場監視機関を指定すべきである。

Member States hold a key role in the application and enforcement of this Regulation. In that respect, each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of this Regulation. Member States may decide to appoint any kind of public entity to perform the tasks of the national competent authorities within the meaning of this Regulation, in accordance with their specific national organisational characteristics and needs. In order to increase organisation efficiency on the side of Member States and to set a single point of contact vis-à-vis the public and other counterparts at Member State and Union levels, each Member State should designate a market surveillance authority to act as a single point of contact.

- (154) 職務権限のある国内機関は、当該機関の活動と職務の客観性の原則を守るため、また、この規則の適用及び実装を確保するため、独立して、公平に、かつ、バイアスなく、当該機関の権限を行使すべきである。それらの機関の構成員は、その構成員の義務と適合しない行動を控えるべきであり、かつ、この規則の下にある機密性の規定に服するべきである。

The national competent authorities should exercise their powers independently, impartially and without bias, so as to safeguard the principles of objectivity of their activities and tasks and to ensure the application and implementation of this Regulation. The members of these authorities should refrain from any action incompatible with their duties and should

be subject to confidentiality rules under this Regulation.

- (155) 高リスク AI システムの提供者が、その提供者の AI システムを改善するための高リスク AI システムの利用上の経験及び設計と開発のプロセスを考慮に入れ得ること、または、あり得る是正の行動を適時の態様で行い得ることを確保するため、全ての提供者は、市場化後監視の制度を設けるべきである。それが関連するときは、市場化後監視は、他の機器及びソフトウェアを含め、他の AI システムとの間のやりとりの分析を含めるべきである。市場化後監視は、法執行機関である設置者の機微の業務運営上のデータを包摂してはならない。この制度は、市場に置かれまたはサービスに供された後にも「学習」し続ける AI システムから生ずることがあり得るリスクがより効率的かつ適時に対処され得ることを確保するための鍵でもある。この文脈において、提供者は、その提供者の AI システムの利用から生ずる重大なインシデント、すなわち、死亡もしくは健康に対する重大な加害、不可欠インフラの運営管理及び運用の重大かつ不可逆的な混乱、基本的な権利を保護することを意図する欧州連合法の下にある義務の違反、または、財産もしくは環境に対する重大な加害を導くインシデントもしくは誤作動を適切な当局に対して報告するための制度を設けることも要求されるべきである。

In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. Where relevant, post-market monitoring should include an analysis of the interaction with other AI systems including other devices and software. Post-market monitoring should not cover sensitive operational data of deployers which are law enforcement authorities. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents resulting from the use of their AI systems, meaning incident or malfunctioning leading to death or serious damage to health, serious and irreversible disruption of the management and operation of critical infrastructure, infringements of obligations under Union law intended to protect fundamental rights or serious damage to property or the environment.

- (156) 欧州連合整合化立法であるこの規則によって定められる要件及び義務の適切かつ実効的な執行を確保するため、規則(EU) 2019/1020 によって設けられた製品の市場監視と遵守の制度は、その全部において適用されるべきである。この規則によって指定された市場監視当局は、この規則及び規則(EU) 2019/1020 の中で定められた全ての執行権限をもつべきであり、かつ、独立して、公平に、かつ、バイアスなく、その当局の権限を行使し、その当局の義務を実行すべきである。AI システムの大多数がこの規則の下にある個別の要件及び義務に服さないとしても、AI システムがリスクを示すときは、市場監視当局は、この規則に従って、全ての AI システムとの関係において措置を講じ得る。この規則の適用範囲内にある欧州連合の機関、部局及び組織の特別の性質のゆえに、それらに関する職務権限のある市場監視当局として、欧州データ保護監督官を指定するのが適切である。このことは、構成国による職務権限のある国内機関の指定を妨げてはならない。市場監視活動は、欧州連合法によってそのような独立性が要求される場合、監視を受ける法主体の職務を独立して実行するためのその法主体の能力に対して影響を与えてはならない。

In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Market surveillance authorities designated pursuant to this Regulation should have all enforcement powers laid down in this Regulation and in Regulation (EU) 2019/1020 and should exercise their powers and carry out their duties independently, impartially and without bias. Although the majority of AI systems are not subject to specific requirements and obligations under this Regulation, market surveillance authorities may take measures in relation to all AI systems when they present a risk in accordance with this Regulation. Due to the specific nature of Union institutions, agencies and bodies falling within the scope of this Regulation, it is appropriate to designate the European Data Protection Supervisor as a competent market surveillance authority for them. This should be without prejudice to the designation of national competent authorities by the Member States. Market surveillance activities should not affect the ability of the supervised entities to carry out their tasks independently, when such independence is required by Union law.

- (157) この規則は、平等性の組織及びデータ保護当局を含め、基本的な権利を保護する欧州連合法の適用を監督する関連国内行政機関または行政組織の能力、職務、権限及び独立性を妨げない。当該行政機関または行政組織の任務のために必要があるときは、それらの機関または組織は、この規則の下において作成された文書へのアクセスももつべきである。健康、安全及び基本的な権利に対するリスクを示す AI システムを対象とする適切かつ適時の執行を確保するため、個別の安全確保手続が定められるべきである。そのようなリスクを示す AI システムに関する手続は、リスクを示す高リスク AI システム、この規則の定められた禁止される実務に違反して市場に置かれ、サービスに供されまたは利用された禁止されたシステム、及び、この規則の中で定められた透明性の要件に違反して利用できるようにされた AI システムであり、かつ、リスクを示すものに対して適用されるべきである。

This Regulation is without prejudice to the competences, tasks, powers and independence of relevant national public authorities or bodies which supervise the application of Union law protecting fundamental rights, including equality bodies and data protection authorities. Where necessary for their mandate, those national public authorities or bodies should also have access to any documentation created under this Regulation. A specific safeguard procedure should be set for ensuring adequate and timely enforcement against AI systems presenting a risk to health, safety and fundamental rights. The procedure for such AI systems presenting a risk should be applied to high-risk AI systems presenting a risk, prohibited systems which have been placed on the market, put into service or used in violation of the prohibited practices laid down in this Regulation and AI systems which have been made available in violation of the transparency requirements laid down in this Regulation and present a risk.

- (158) 欧州連合金融サービス法は、そのサービスが AI システムを活用する場合を含め、そのサービスの提供の過程において規律される金融機関に対して適用可能な内部統制及びリスク管理の規定及び要件を含んでいる。この規則の下における義務並びに欧州連合の金融サービスの法行為の関連規定及び要件の一貫性のある適用と執行を確保するため、構成国の市場監視の職務を満たすために構成国が別の機関を指定しない限り、規律されまたは監督を受ける金融機関によって提供されまたは利用される AI システムに関し、市場監視活動の目的の場合を含め、この規則の実装を監督する目的のための職務権限のある機関として、それらの機関それぞれの職務権限の範囲内において、

それらの法行為の監督及び執行に関する職務権限のある機関、とりわけ、欧州議会及び理事会の規則(EU) No 575/2013⁴⁶並びに欧州議会及び理事会の指令 2008/48/EC⁴⁷, 指令 2009/138/EC⁴⁸, 指令 2013/36/EU⁴⁹, 指令 2014/17/EU⁵⁰及び指令(EU) 2016/97⁵¹に定義する職務権限のある機関が指定されるべきである。それらの職務権限のある機関は、欧州連合の関連する金融サービス法の下にある職務権限のある機関の現行の監督の仕組み及び手続にしかるべく統合され得る事後の市場監視活動を実施するための権限を含め、この規則の要件及び義務を執行するため、この規則及び規則(EU) 2019/1020 の下にある全ての権限をもつべきである。この規則の下にある市場監視当局として行動する場合、指令 2013/36/EU の下において規律される与信機関の監督に関する職責を負う国内機関であって、理事会規則 No 1024/2013⁵²によって設置された単一の監視の仕組みに参加する機関が、欧州中央銀行に対し、その機関の市場監視活動の過程において発見され、同規則の中で細目が定められた欧州中央銀行の健全性監督の職務にとって潜在的に影響をもち得る情報を遅滞なく報告すべきであることを予定するのが適切である。この規則と、指令 2013/36/EU の下において規律される与信機関に適用可能な諸規定との間の一貫性を更に拡大するため、リスク管理、市場化後監視及

⁴⁶ 与信機関及び投資企業の健全性要件に関する、並びに、規則(EU) No 648/2012を改正する欧州議会及び理事会の 2013 年 6 月 26 日の規則(EU) No 575/2013 (OJ L 176, 27.6.2013, p. 1).

Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

⁴⁷ 消費者向け与信合意に関する及び理事会指令 87/102/EEC を廃止する欧州議会及び理事会の 2008 年 4 月 23 日の指令 2008/48/EC (OJ L 133, 22.5.2008, p. 66).

Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L 133, 22.5.2008, p. 66).

⁴⁸ 保険及び再保険の事業の開始及び遂行に関する欧州議会及び理事会の 2009 年 11 月 25 日の指令 2009/138/EC (Solvency II) (OJ L 335, 17.12.2009, p. 1).

Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

⁴⁹ 与信機関の活動へのアクセス並びに与信機関及び投資企業の健全性監督に関する、指令 2002/87/EC を改正し、指令 2006/48/EC 及び指令 2006/49/EC を廃止する欧州議会及び理事会の 2013 年 6 月 26 日の指令 2013/36/EU (OJ L 176, 27.6.2013, p. 338).

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

⁵⁰ 居住用不動産と関連する消費者向け与信合意に関する、並びに、指令 2008/48/EC, 指令 2013/36/EU 及び規則(EU) No 1093/2010 を改正する欧州議会及び理事会の 2014 年 2 月 4 日の指令 2014/17/EU (OJ L 60, 28.2.2014, p. 34).

Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 60, 28.2.2014, p. 34).

⁵¹ 保険の販売に関する欧州議会及び理事会の 2016 年 1 月 20 日の指令(EU) 2016/97 (OJ L 26, 2.2.2016, p. 19).

Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19).

⁵² 与信機関の健全性監督と関連する基本方針に関し欧州中央銀行に特別の職務を与える 2013 年 10 月 15 日の理事会規則(EU) No 1024/2013 (OJ L 287, 29.10.2013, p. 63).

Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

び文書化と関係する提供者の事務上の義務中の幾つかを指令 2013/36/EU の下にある既存の義務及び手続の中に統合することも適切である。重複を避けるため、指令 2013/36/EU によって規律される与信機関に適用されるものの範囲内において、高リスク AI システムの提供者の品質管理システム及びその設置者に課される監視義務と関係して、限定的な適用除外も予定されるべきである。金融部門における一般性と平等な取扱いを確保するため、指令 2009/138/EC の下にある保険事業者、再保険事業者及び保険持株会社に対し、指令(EU) 2016/97 の下にある保険仲介事業者に対し、並びに、それ以外のタイプの、欧州連合の関連金融サービス法により設けられた内部統制、約定またはプロセスと関連する要件に服する金融機関に対し、同じ制度が適用されるべきである。

Union financial services law includes internal governance and risk-management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legal acts, the competent authorities for the supervision and enforcement of those legal acts, in particular competent authorities as defined in Regulation (EU) No 575/2013 of the European Parliament and of the Council⁽⁴⁶⁾ and Directives 2008/48/EC⁽⁴⁷⁾, 2009/138/EC⁽⁴⁸⁾, 2013/36/EU⁽⁴⁹⁾, 2014/17/EU⁽⁵⁰⁾ and (EU) 2016/97⁽⁵¹⁾ of the European Parliament and of the Council, should be designated, within their respective competences, as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions unless Member States decide to designate another authority to fulfil these market surveillance tasks. Those competent authorities should have all powers under this Regulation and Regulation (EU) 2019/1020 to enforce the requirements and obligations of this Regulation, including powers to carry out ex post market surveillance activities that can be integrated, as appropriate, into their existing supervisory mechanisms and procedures under the relevant Union financial services law. It is appropriate to envisage that, when acting as market surveillance authorities under this Regulation, the national authorities responsible for the supervision of credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism established by Council Regulation (EU) No 1024/2013⁽⁵²⁾, should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in that Regulation. To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU, it is also appropriate to integrate some of the providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on deployers of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU. The same regime should apply to insurance and re-insurance undertakings and insurance holding companies under Directive 2009/138/EC and the insurance intermediaries under Directive (EU) 2016/97 and other types of financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services law to ensure consistency and equal treatment in the financial sector.

- (159) 生体要素の分野における高リスク AI システムに関する各市場監視当局は、この規則の別紙の中に列挙されているように、それらのシステムが法執行、移民、難民及び出入国管理または法務及び民

主的な過程の運営の目的のために利用される範囲内において、少なくとも、処理されている全ての個人データにアクセスする権限及びその当局の職務の遂行のために必要な全ての情報へのアクセスを得る権限を含め、実効的な調査権限及び是正権限をもつべきである。市場監視当局は、完全な独立性をもって行動することにより、その当局の権限を行使できるべきである。この規則の下にある機微の業務運営上のデータへのその当局のアクセスの制限は、指令(EU) 2016/680 によってその当局に対して与えられた権限を妨げてはならない。この規則の下にある国内データ保護当局に対するデータの開示に関する適用除外は、この規則の適用範囲の外にあるその当局の現在の権限または将来の権限に対して影響を与えてはならない。

Each market surveillance authority for high-risk AI systems in the area of biometrics, as listed in an annex to this Regulation insofar as those systems are used for the purposes of law enforcement, migration, asylum and border control management, or the administration of justice and democratic processes, should have effective investigative and corrective powers, including at least the power to obtain access to all personal data that are being processed and to all information necessary for the performance of its tasks. The market surveillance authorities should be able to exercise their powers by acting with complete independence. Any limitations of their access to sensitive operational data under this Regulation should be without prejudice to the powers conferred to them by Directive (EU) 2016/680. No exclusion on disclosing data to national data protection authorities under this Regulation should affect the current or future powers of those authorities beyond the scope of this Regulation.

- (160) 市場監視当局及び欧州委員会は、共同調査を含め、複数の市場監視当局により実施されまたは市場管理当局と欧州委員会との共同で実施され、複数の構成国にわたる重大なリスクを示すと判断されている特定の類型の高リスク AI システムに関し、この規則との関係において、遵守を促進し、不遵守を発見し、認識を向上させ、及び、指針を提供することを狙いとしても共同活動を提案できるべきである。遵守を向上させるための共同活動は、規則(EU) 2019/1020 の第 9 条に従って実施されるべきである。AI 総局は、共同調査のための調整の支援を提供すべきである。

The market surveillance authorities and the Commission should be able to propose joint activities, including joint investigations, to be conducted by market surveillance authorities or market surveillance authorities jointly with the Commission, that have the aim of promoting compliance, identifying non-compliance, raising awareness and providing guidance in relation to this Regulation with respect to specific categories of high-risk AI systems that are found to present a serious risk across two or more Member States. Joint activities to promote compliance should be carried out in accordance with Article 9 of Regulation (EU) 2019/1020. The AI Office should provide coordination support for joint investigations.

- (161) 一般目的 AI モデルを基礎としている AI システムに関する欧州連合レベル及び国内レベルの職責及び職務権限を明確にする必要がある。職務権限の重複を避けるため、AI システムが一般目的 AI モデルを基礎としており、かつ、そのモデルとシステムが同一の提供者から提供されている場合、その監督は、欧州連合レベルで AI 総局を通じて行われる。AI 総局は、この目的のために、規則(EU) 2019/1020 の意味における市場監視当局の権限をもつべきである。それ以外の全ての場合において、国内市場監視当局は、AI システムの監視に関する職責を維持する。ただし、少なくとも 1 つの高リスク

クとして分類される目的のために設置者によって直接に利用され得る一般目的 AI システムに関しては、市場監視当局は、遵守の評価を実施するために AI 総局と協力すべきであり、かつ、委員会及び他の市場監視当局に対し、しかるべく連絡すべきである。更に、それを基礎として当該高リスク AI システムが構築されている一般目的 AI モデルに関する一定の情報に対して当該市場監視当局がアクセスできないために、その市場監視当局が高リスク AI システムの調査を完了できないときは、その市場監視当局は、AI 総局に対して補助を要請できるべきである。そのような場合、規則(EU) 2019/1020 の第VI章の国境を越える案件における相互補助に関する手続が類推して適用されるべきである。

It is necessary to clarify the responsibilities and competences at Union and national level as regards AI systems that are built on general-purpose AI models. To avoid overlapping competences, where an AI system is based on a general-purpose AI model and the model and system are provided by the same provider, the supervision should take place at Union level through the AI Office, which should have the powers of a market surveillance authority within the meaning of Regulation (EU) 2019/1020 for this purpose. In all other cases, national market surveillance authorities remain responsible for the supervision of AI systems. However, for general-purpose AI systems that can be used directly by deployers for at least one purpose that is classified as high-risk, market surveillance authorities should cooperate with the AI Office to carry out evaluations of compliance and inform the Board and other market surveillance authorities accordingly. Furthermore, market surveillance authorities should be able to request assistance from the AI Office where the market surveillance authority is unable to conclude an investigation on a high-risk AI system because of its inability to access certain information related to the general-purpose AI model on which the high-risk AI system is built. In such cases, the procedure regarding mutual assistance in cross-border cases in Chapter VI of Regulation (EU) 2019/1020 should apply *mutatis mutandis*.

- (162) 集中化された欧州連合の専門知識の利用と欧州連合レベルの波及効果を最善にするため、一般目的 AI モデルの提供者に対して課される義務の監督権限及び執行権限は、欧州委員会の職務権限であるべきである。AI 総局は、一般目的 AI モデルと関連するこの規則の実効的な実装を監視するために必要となる全ての行動を実施できるべきである。AI 総局は、その監視活動の結果に従って AI 総局自身の発意により、または、この規則に定める条件に沿って市場監視当局からの要請に基づき、一般目的 AI モデルの提供者に関し、規定違反の可能性のある行為を調査できるべきである。AI 総局の実効的な監視を支えるため、一般目的 AI モデル及び一般目的 AI システムの提供者に関する規定の違反の可能性のある行為に関する苦情を下流の提供者が申立て得ることが定められるべきである。

To make best use of the centralised Union expertise and synergies at Union level, the powers of supervision and enforcement of the obligations on providers of general-purpose AI models should be a competence of the Commission. The AI Office should be able to carry out all necessary actions to monitor the effective implementation of this Regulation as regards general-purpose AI models. It should be able to investigate possible infringements of the rules on providers of general-purpose AI models **both** on its own initiative, following the results of its monitoring activities, or upon request from market surveillance authorities in line with the conditions set out in this Regulation. To support effective monitoring of the AI Office, it should provide for the possibility that downstream providers lodge complaints about possible

infringements of the rules on providers of general-purpose AI models and systems.

- (163) 一般目的 AI モデルの統治制度を補完するという観点から、科学パネルは、AI 総局の監視活動を支えるべきであり、また、一定の場合において、AI 総局に対し、調査のような事後対応の引き金となる該当性あり警報を提供できる。一般目的 AI モデルが欧州連合レベルで具体的かつ識別可能なリスクを呈していると疑うべき根拠を科学パネルがもつ場合が、そのような場合であるべきである。更に、ある一般目的 AI モデルが、システミックリスクをもつ一般目的 AI モデルとしての分類を導く基準に適合していると疑うべき根拠を科学パネルがもつ場合が、そのような場合であるべきである。科学パネルがその職務の遂行のために必要となる情報を具備するため、提供者に対して文書または情報を要求することを科学パネルが欧州委員会に対して要請できる仕組みが存在すべきである。

With a view to complementing the governance systems for general-purpose AI models, the scientific panel should support the monitoring activities of the AI Office and may, in certain cases, provide qualified alerts to the AI Office which trigger follow-ups, such as investigations. This should be the case where the scientific panel has reason to suspect that a general-purpose AI model poses a concrete and identifiable risk at Union level. Furthermore, this should be the case where the scientific panel has reason to suspect that a general-purpose AI model meets the criteria that would lead to a classification as general-purpose AI model with systemic risk. To equip the scientific panel with the information necessary for the performance of those tasks, there should be a mechanism whereby the scientific panel can request the Commission to require documentation or information from a provider.

- (164) AI 総局は、この規則の中で定められた一般目的 AI モデルの提供者の義務の実効的な実装と遵守を監視するために必要となる行動をとり得るべきである。AI 総局は、文書及び情報を要求することによる場合、評価を実施することによる場合、並びに、一般目的 AI モデルの提供者に対して対策を要求することによる場合を含め、この規則の中で定められた権限に従って、違反の可能性のある行為を調査できるべきである。評価を実施する際、独立の専門知識を活用するため、AI 総局は、AI 総局の代わりに評価を実施するための独立の専門家を関与させ得るべきである。義務の遵守は、就中、特定されたシステミックリスクの場合においてはリスクを緩和する方策を含め、適切な対策をとることを要求することを通じて、また、そのモデルを市場において利用できることを制限し、回収し、または、リコールすることを要求することを通じて、執行可能であるべきである。この規則の中で定められた手続上の権利を超える必要がある場合における安全確保として、一般目的 AI モデルの提供者は、規則 (EU) 2019/1020 の第 18 条に定める手続上の権利をもつべきである。同権利は、この規則によって定められるより細目的な手続上の権利を妨げることなく、類推して適用されるべきである。

The AI Office should be able to take the necessary actions to monitor the effective implementation of and compliance with the obligations for providers of general-purpose AI models laid down in this Regulation. The AI Office should be able to investigate possible infringements in accordance with the powers provided for in this Regulation, including by requesting documentation and information, by conducting evaluations, as well as by requesting measures from providers of general-purpose AI models. When conducting evaluations, in order to make use of independent expertise, the AI Office should be able to involve independent experts to carry out the evaluations on its behalf. Compliance with the obligations should be enforceable, inter alia, through requests to take appropriate measures, including risk mitigation

measures in the case of identified systemic risks as well as restricting the making available on the market, withdrawing or recalling the model. As a safeguard, where needed beyond the procedural rights provided for in this Regulation, providers of general-purpose AI models should have the procedural rights provided for in Article 18 of Regulation (EU) 2019/1020, which should apply *mutatis mutandis*, without prejudice to more specific procedural rights provided for by this Regulation.

- (165) この規則の要件に従った高リスク AI システム以外の AI システムの開発は、欧州連合内における倫理に適った信頼性のある AI の、より大きな導入を導き得る。高リスクではない AI システムの提供者は、統治の仕組みと関連する行動準則を含め、高リスク AI システムに適用可能な強行的な要件の全部または一部の任意の適用を育成することを意図し、そのシステムの所期の目的及びそれに含まれるより低度のリスクに照らして調整され、かつ、モデル及びデータカードのような利用可能な技術上のソリューション及び産業上のベストプラクティスを考慮に入れた行動準則を作成することが推奨されるべきである。高リスクであるかどうかを問わず AI システム及び AI モデルの提供者、並びに、しかるべく、その設置者は、例えば、信頼できる AI のための欧州倫理指針の諸要素、環境の持続性、AI リテラシーの諸方策、脆弱な者への配慮及び障害をもつ者のアクセシビリティを含め社会包摂的かつ多様性のある AI システムの設計及び開発、企業団体と市民社会団体、学术界と調査研究団体、労働組合と消費者保護団体のような適格な利害関係者の AI システムの設計及び開発へのしかるべき関与を伴う利害関係者の参加、並びに、ジェンダーバランスを含め開発チームの多様性という諸要素と関連する付加的な要件を任意で適用することも推奨されるべきである。任意の行動準則が実効的であることを確保するため、任意の行動準則は、明確な目標及びその目標の達成を測定するための鍵となる遂行能力指標を基礎とすべきである。任意の行動準則はまた、しかるべく、企業団体と市民社会団体、学术界、調査研究団体、労働組合と消費者保護団体のような適格な利害関係者の関与を伴う社会包摂的な方法で策定されるべきである。欧州委員会は、部門別の性質のものを含め、データアクセスインフラ、異なるタイプのデータの意味論上及び技術上の相互運用性に関するものを含め、AI 開発のための国境を越えるデータ交換を妨げず技術上の障壁を低くすることを容易にするための取組みを進展させ得る。

The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of ethical and trustworthy AI in the Union. Providers of AI systems that are not high-risk should be encouraged to create codes of conduct, including related governance mechanisms, intended to foster the voluntary application of some or all of the mandatory requirements applicable to high-risk AI systems, adapted in light of the intended purpose of the systems and the lower risk involved and taking into account the available technical solutions and industry best practices such as model and data cards. Providers and, as appropriate, deployers of all AI systems, **high-risk or not**, and AI models should also be encouraged to apply on a voluntary basis additional requirements related, for example, to the elements of the Union's Ethics Guidelines for Trustworthy AI, environmental sustainability, AI literacy measures, inclusive and diverse design and development of AI systems, including attention to vulnerable persons and accessibility to persons with disability, stakeholders' participation with the involvement, as appropriate, of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisations in the design and development of AI systems, and diversity of the development teams, including gender balance. To ensure that the voluntary codes of conduct are effective, they should be based on

clear objectives and key performance indicators to measure the achievement of those objectives. They should also be developed in an inclusive way, as appropriate, with the involvement of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisation. The Commission may develop initiatives, including of a sectoral nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.

- (166) この規則に従って高リスクではなく、そして、高リスク AI システムに関して定める要件の遵守を要求されない製品と関連する AI システムが、それでもなお、市場に置かれた場合はサービスに供される際には安全であることが重要である。この目的に貢献するため、欧州議会及び理事会の規則(EU) 2023/988⁵³が安全網として適用されるだろう。

It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out for high-risk AI systems are nevertheless safe when placed on the market or put into service. To contribute to this objective, Regulation (EU) 2023/988 of the European Parliament and of the Council⁽⁵³⁾ would apply as a safety net.

- (167) 欧州連合レベル及び国内レベルの職務権限のある機関の信頼に満ち建設的な協力を確保するため、この規則の適用に関与する全ての関係者は、欧州連合法及び国内法に従い、当該関係者の職務を実施する際に入手した情報及びデータの機密性を尊重すべきである。それらの関係者は、とりわけ、知的財産権、企業の機密情報及び営業秘密、この規則の実効的な実装、公共の利益及び国家安全保障上の利益、刑事手続及び行政手続の完全性並びに機密情報の完全性を保護するような態様で、それらの関係者の職務及び活動を実施すべきである。

In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks, in accordance with Union or national law. They should carry out their tasks and activities in such a manner as to protect, in particular, intellectual property rights, confidential business information and trade secrets, the effective implementation of this Regulation, public and national security interests, the integrity of criminal and administrative proceedings, and the integrity of classified information.

- (168) この規則の遵守は、制裁及びそれ以外の執行措置を科すという手段によって執行されるべきである。構成国は、この規則の条項の違反行為に対する実効的であり、比例的であり、かつ、抑止力のある

⁵³ 一般的な製品の安全性に関する、欧州議会及び理事会の規則(EU) No 1025/2012、欧州議会及び理事会の指令(EU) 2020/1828 を改正する、並びに、欧州議会及び理事会の指令 2001/95/EC、理事会指令 87/357/EEC を廃止する欧州議会及び理事会の 2023 年 5 月 10 日の規則(EU)2023/988(OJ L135, 23.5.2023, p. 1).

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).

制裁を定めることによる場合を含め、かつ、一事不再理の原則を尊重して、この規則の条項が実装されることを確保するために必要となる全ての措置を講ずるべきである。この規則の違反行為に対する行政上の制裁を強化しかつ整合化するため、一定の個別の違反行為に対する行政上の制裁金を設けるための上限が定められるべきである。制裁金の額を評価検討する際、構成国は、個々の具体的な案件において、とりわけ当該違反行為及びその結果の性質、重大性及び持続期間を適切に考慮し、また、とりわけ当該提供者がスタートアップを含め SMEs であるときは、提供者の規模を適切に考慮して、個別の状況の関連する全ての事情を考慮に入れるべきである。欧州データ保護監督官は、この規則の適用範囲内にある欧州連合の機関、部局及び組織に対して制裁金を科す権限をもつべきである。

Compliance with this Regulation should be enforceable by means of the imposition of penalties and other enforcement measures. Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement, and to respect the *ne bis in idem* principle. In order to strengthen and harmonise administrative penalties for infringement of this Regulation, the upper limits for setting the administrative fines for certain specific infringements should be laid down. When assessing the amount of the fines, Member States should, in each individual case, take into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and to the size of the provider, in particular if the provider is an SME, including a start-up. The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation.

- (169) この規則の下において一般目的 AI モデルの提供者に対して課される義務の遵守は、就中、制裁金という手段によって執行可能であるべきである。その目的のために、この規則に従って欧州委員会から要求され、比例性の原則に従った適正な制限期間に服する措置の不遵守を含め、それらの義務の違反行為に関しても適切なレベルの制裁金が定められるべきである。この規則の下において欧州委員会によって行われる全ての決定は、TFEU の第 261 条による司法裁判所の制裁と関連する無限定の裁判管轄権を含め、欧州連合の司法裁判所による TFEU に従った見直しに服する。

Compliance with the obligations on providers of general-purpose AI models imposed under this Regulation should be enforceable, inter alia, by means of fines. To that end, appropriate levels of fines should also be laid down for infringement of those obligations, including the failure to comply with measures requested by the Commission in accordance with this Regulation, subject to appropriate limitation periods in accordance with the principle of proportionality. All decisions taken by the Commission under this Regulation are subject to review by the Court of Justice of the European Union in accordance with the TFEU, including the unlimited jurisdiction of the Court of Justice with regard to penalties pursuant to Article 261 TFEU.

- (170) 欧州連合法及び国内法は、AI システムの利用によって当該の者の権利及び自由が負の影響を受けている自然人及び法人に対し、実効的な救済を既に提供している。それらの救済を妨げることなく、この規則の違反行為があったと考える根拠をもつ自然人または法人は、関連する市場監視当局に対し、苦情を申立てる資格を与えられるべきである。

Union and national law already provide effective remedies to natural and legal persons whose rights and freedoms are adversely affected by the use of AI systems. Without prejudice to those remedies, any natural or legal person that has grounds to consider that there has been an infringement of this Regulation should be entitled to lodge a complaint to the relevant market surveillance authority.

- (171) 設置者の判定が、この規則の適用範囲内にある一定の高リスク AI システムからの出力を主として基礎としている場合であり、かつ、当該判定が、当該影響を受ける個人の健康、安全または基本的な権利に対して負の影響を与えているとそれらの個人が考えるような方法で、それらの個人の法律上の影響を生成または同様の重大な影響を生成している場合、影響を受ける個人は、説明を得る権利をもつべきである。その説明は、明確で意味のあるものであるべきであり、かつ、影響を受ける個人がそれらの個人の権利を行使できる根拠を提供すべきである。説明を得る権利は、欧州連合法または国内法の適用除外または制限に服する AI システムの利用に対して適用してはならず、また、その権利が欧州連合法の下において既に定められていない範囲内に限り、適用されるべきである。

Affected persons should have the right to obtain an explanation where a deployer's decision is based mainly upon the output from certain high-risk AI systems that fall within the scope of this Regulation and where that decision produces legal effects or similarly significantly affects those persons in a way that they consider to have an adverse impact on their health, safety or fundamental rights. That explanation should be clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights. The right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions follow from Union or national law and should apply only to the extent this right is not already provided for under Union law.

- (172) この規則の違反行為に関して内部告発者として行動する個人は、欧州連合法の下において保護されるべきである。それゆえ、欧州議会及び理事会の指令(EU) 2019/1937⁵⁴は、この規則の違反行為の通報及びそのような違反行為を通報する個人の保護に対して適用されるべきである。

Persons acting as whistleblowers on the infringements of this Regulation should be protected under the Union law. Directive (EU) 2019/1937 of the European Parliament and of the Council⁽⁵⁴⁾ should therefore apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

- (173) 法制枠組みが必要に応じて調整され得ることを確保するため、AI システムが高リスクであると判断されない場合の条件、高リスク AI システムのリスト、技術文書と関連する条項、EU 適合性宣言書の内容、適合性評価手続と関連する条項、品質管理システムの評価及び技術文書の評価を基礎とする適合性評価手続が適用されるべき高リスク AI システムを定める条項、当該ベンチマーク及び指標を補遺することによる場合を含め、システミックリスクをもつ一般目的 AI モデルの分類に関する規定の

⁵⁴ 欧州連合法の違反を通報する個人の保護に関する欧州議会及び理事会の 2019 年 10 月 23 日の指令(EU) 2019/1937 (OJ L305, 26.11.2019, p. 17).

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L305, 26.11.2019, p. 17).

中にある閾値、ベンチマーク及び指標、システミックリスクをもつ一般目的 AI モデルの指定のための基準、一般目的 AI モデルの提供者のための技術文書、一般目的 AI モデルの提供者のための透明性情報を改正するために TFEU の第 290 条に従って法行為を採択する権限は、欧州委員会に対して委任されるべきである。その準備作業の間、専門家レベルのものを含め、欧州委員会が適切な意見聴取を実施すること、及び、より良い立法に関する 2016 年 4 月 13 日の機関間合意⁵⁵に定める基本原則に従ってそれらの意見聴取が行われることは、特に重要なことである。とりわけ、委任される行為の準備への平等な参加を確保するため、欧州議会及び理事会は、構成国の専門家と同時に全ての文書を受領し、かつ、構成国の専門家は、自動的に、委任される行為の準備を取り扱う欧州委員会の専門家グループの会合へのアクセスをもつ。

In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the conditions under which an AI system is not to be considered to be high-risk, the list of high-risk AI systems, the provisions regarding technical documentation, the content of the EU declaration of conformity the provisions regarding the conformity assessment procedures, the provisions establishing the high-risk AI systems to which the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply, the threshold, benchmarks and indicators, including by supplementing those benchmarks and indicators, in the rules for the classification of general-purpose AI models with systemic risk, the criteria for the designation of general-purpose AI models with systemic risk, the technical documentation for providers of general-purpose AI models and the transparency information for providers of general-purpose AI models. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making⁵⁵. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

- (174) 技術の急速な発展及びこの規則を実効的に適用するために要求される技術上の専門知識に鑑み、欧州委員会は、2029 年 8 月 2 日までに及びその後は 4 年毎に、この規則を評価し、見直すべきであり、かつ、欧州議会及び理事会に対して報告すべきである。加えて、この規則の適用範囲の内容を考慮に入れた上で、欧州委員会は、年 1 回、高リスク AI システムのリスト及び禁止される実務のリストを改正する必要性の有無の評価を実施すべきである。それに加えて、2028 年 8 月 2 日までに及びその後は 4 年毎に、欧州委員会は、別の措置または活動の必要性の有無を含め、この規則の別紙中の高リスク分野の表題のリスト、透明性義務の適用範囲内にある AI システム、監視と統治の制度の実効性、並びに、一般目的 AI モデルのエネルギー効率の良い開発に関する標準化派生物策定の進捗状況を見直す必要性の有無に関して評価すべきであり、かつ、欧州議会及び理事会に対して報告すべきである。最後に、2028 年 8 月 2 日までに及びその後は 3 年毎に、欧州委員会は、高リスク AI システム以外の AI システムの場合において高リスク AI システムに関する要件の適用及び

⁵⁵ OJL 123, 12.5.2016, p. 1.

そのような AI システムに関するそれ以外のあり得る付加的要件の適用を促進するための任意の行動準則の影響及び実効性を評価すべきである。

Given the rapid technological developments and the technical expertise required to effectively apply this Regulation, the Commission should evaluate and review this Regulation by 2 August 2029 and every four years thereafter and report to the European Parliament and the Council. In addition, taking into account the implications for the scope of this Regulation, the Commission should carry out an assessment of the need to amend the list of high-risk AI systems and the list of prohibited practices once a year. Moreover, by 2 August 2028 and every four years thereafter, the Commission should evaluate and report to the European Parliament and to the Council on the need to amend the list of high-risk areas **headings** in the annex to this Regulation, the AI systems within the scope of the transparency obligations, the effectiveness of the supervision and governance system and the progress on the development of standardisation deliverables on energy efficient development of general-purpose AI models, including the need for further measures or actions. Finally, by 2 August 2028 and every three years thereafter, the Commission should evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements provided for high-risk AI systems in the case of AI systems other than high-risk AI systems and possibly other additional requirements for such AI systems.

- (175) この規則の実装のための統一的な条件を確保するため、実装権限は、欧州委員会に対して与えられるべきである。それらの権限は、欧州議会及び理事会の規則(EU) No 182/2011⁵⁶に従って行使されるべきである。

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council⁵⁶.

- (176) この規則の目的、すなわち、欧州連合内の AI システム及びそれを支える技術革新の危険な影響に抗して、健康、安全、並びに、民主主義、法の支配及び環境保護を含め、憲章に掲げられた基本的な権利の高いレベルの保護を確保しつつ、域内市場の稼働を向上させること及び人間中心であり信頼できる AI の導入を促進することは、構成国によっては十分に達成され得ず、その活動の規模または影響のゆえに、欧州連合レベルでより良く達成され得るので、欧州連合は、TEU の第 5 条に定める補完性の原則に従い、措置を採択できる。同条に定める比例性の原則に従い、この規則は、その目的を達成するために必要なところを超えることがない。

⁵⁶ 欧州委員会の実装権限の行使の構成国による監督のための仕組みに関する規定及び基本原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011 (OJL55, 28.2.2011, p. 13).

Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJL55, 28.2.2011, p. 13).

Since the objective of this Regulation, namely to improve the functioning of the internal market and to promote the uptake of human centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection against harmful effects of AI systems in the Union and supporting innovation, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

- (177) 法的確実性を確保するため、運営者のための適切な適応期間を確保するため、及び、AI システムの利用の継続性を確保することによる場合を含め、市場の混乱を避けるため、当該 AI システムが当該の日から当該システムの設計または所期の目的において大きな修正に服する場合に限り、この規則の全体的な適用の日よりも前に市場に置かれまたはサービスに供された高リスク AI システムに対してこの規則を適用することが適切である。この点に関し、この規則により高リスク AI システムのみと関連して用いられる実質的な修正の概念とその実質において同一の概念として大きな修正の概念が理解されるべきことを明確にすることが適切である。例外的に、かつ、公衆への説明責任に照らし、この規則の別紙の中に列挙される法行為によって設けられた大規模 IT システムのコンポーネントである AI システムの運用者及び行政機関によって利用されることを意図する高リスク AI システムの運用者は、それぞれ 2030 年の最終日まで及び 2030 年 8 月 2 日までに、この規則の要件を遵守するために必要となる手立てを講ずるべきである。

In order to ensure legal certainty, ensure an appropriate adaptation period for operators and avoid disruption to the market, including by ensuring continuity of the use of AI systems, it is appropriate that this Regulation applies to the high-risk AI systems that have been placed on the market or put into service before the general date of application thereof, only if, from that date, those systems are subject to significant changes in their design or intended purpose. It is appropriate to clarify that, in this respect, the concept of significant change should be understood as equivalent in substance to the notion of substantial modification, which is used with regard only to high-risk AI systems pursuant to this Regulation. On an exceptional basis and in light of public accountability, operators of AI systems which are components of the large-scale IT systems established by the legal acts listed in an annex to this Regulation and operators of high-risk AI systems that are intended to be used by public authorities should, respectively, take the necessary steps to comply with the requirements of this Regulation by end of 2030 and by 2 August 2030.

- (178) 高リスク AI システムの提供者は、移行期間中であっても、この規則の関連義務の遵守を任意に開始することが推奨される。

Providers of high-risk AI systems are encouraged to start to comply, on a voluntary basis, with the relevant obligations of this Regulation **already** during the transitional period.

- (179) この規則は、2026 年 8 月 2 日から適用されるべきである。ただし、一定の方法による AI の利用と関係する許容し難いリスクを考慮し、この規則の禁止条項及び総則的な条項は、その日の前であって

も、2025 年 2 月 2 日から適用されるべきである。それらの禁止の完全な効果が発生するのはこの規則の統治及び執行が確立された後であるとはいえ、その禁止の適用を想定することは、許容し難いリスクを考慮に入れるために、また、民事法のような別の手続において効力をもつために、重要なことである。それに加えて、統治及び適合性評価制度と関連するインフラは、2026 年 8 月 2 日より前に運用開始となっているべきであり、それゆえ、指定組織及び統治の構造に関する条項は、2025 年 8 月 2 日から適用されるべきである。技術の発展と一般目的 AI モデルの導入の急速なペースに鑑み、一般目的 AI モデルの提供者の義務は、2025 年 8 月 2 日から適用されるべきである。提供者が期限までにその遵守を説明できるようにするため、実務準則は、2025 年 5 月 2 日までに準備されるべきである。AI 総局は、技術の発展に照らして分類の基準と手続が最新のものであることを確保すべきである。加えて、構成国は、行政上の制裁金を含め、制裁に関する規定を定め、欧州委員会に対してそれを通知すべきであり、かつ、この規則の適用の日までにこれらの規定が適正かつ実効的に実装されることを確保すべきである。それゆえ、制裁に関する条項は、2025 年 8 月 2 日から適用されるべきである。

This Regulation should apply from 2 August 2026. However, taking into account the unacceptable risk associated with the use of AI in certain ways, the prohibitions as well as the general provisions of this Regulation should **already** apply from 2 February 2025. While the full effect of those prohibitions follows with the establishment of the governance and enforcement of this Regulation, anticipating the application of the prohibitions is important to take account of unacceptable risks and to have an effect on other procedures, such as in civil law. Moreover, the infrastructure related to the governance and the conformity assessment system should be operational before 2 August 2026, therefore the provisions on notified bodies and governance structure should apply from 2 August 2025. Given the rapid pace of technological advancements and adoption of general-purpose AI models, obligations for providers of general-purpose AI models should apply from 2 August 2025. Codes of practice should be ready by 2 May 2025 in view of enabling providers to demonstrate compliance on time. The AI Office should ensure that classification rules and procedures are up to date in light of technological developments. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on penalties should apply from 2 August 2025.

- (180) 欧州データ保護監督官及び欧州データ保護委員会は、規則(EU) 2018/1725 の第 42 条第 1 項及び第 2 項に従って意見聴取を受け、2021 年 6 月 18 日にその共同意見書を伝達した、

The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered their joint opinion on 18 June 2021,

以上のとおりであるので、この規則を採択する:

HAVE ADOPTED THIS REGULATION:

2024 Printed in Japan

ISSN 2432-6089

法と情報雑誌 第9巻第3号 (通巻第57号)

The Law and Information Magazine vol.9 no.3 (consecutive no.57)

2024年8月31日発行

2024年10月19日誤記等修正版発行

発行者 夏井高人

発行所 法と情報研究会 (代表 夏井高人)

東京都千代田区神田駿河台1-1

学校法人明治大学研究棟

(非売品)