REGUL ATION (EU) 2024/1689 OF THE EUR OPEAN 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 Directiv es 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) THE EUR OPEAN PARLIAMENT AND THE COUNCIL OF THE EUR OPEAN 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 draf t legislative act to the national parliaments, Having regard to the opinion of the European Economic and Social Committe e (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 ordinar y legislative procedure (4), Whereas: (1) The purpose of this Regulation is to imp rove the functioning of the internal marke t by laying down a unif orm legal framew ork in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence syste ms (AI systems) in the Union, in accordance with Union values, to promote the uptak e of human centr ic and trustwor thy artificial intellig ence (AI) while ensur ing a high level of prot ection of health, safety, fundamental rights as enshr ined in the Char ter of Fundamental Rights of the European Union (the ‘Char ter’), including democracy , the rule of law and environmental prot ection, to protect against the harmful effects of AI syste ms in the Union, and to suppor t inno vation. This Regulation ensures the free moveme nt, cross-border , of AI-based goods and services, thus preventing Member States from imp osing restr ictions on the development, mark eting and use of AI systems, unless explicitly author ised by this Regulation. (2) This Regulation should be applied in accordance with the values of the Union enshr ined as in the Char ter, facilitating the protection of natural persons, under takings, democracy , the rule of law and environmental prot ection, while boosting innovation and emplo yment and making the Union a leader in the uptake of trustwo rthy AI. (3) AI systems can be easily deplo yed in a large variety of sectors of the economy and many parts of society , including across borders, and can easily circulat e throughout the Union. Certain Member States have already explored the adop tion of national rules to ensure that AI is trustwor thy and safe and is developed and used in accordance with fundamental rights obliga tions. Diverging national rules may lead to the fragmentation of the inter nal market and may decrease legal certainty for operators that develop, import or use AI systems. A consistent and high level of prot ection throughout the Union should theref ore be ensured in order to achi eve trustw orthy AI, while divergence s ham pering the free circulation, inno vation, deplo yment and the uptak e of AI systems and related products and services within the inter nal marke t should be prevent ed by laying down unif orm obligations for operato rs and Offi cial Jour nal of the European UnionEN L series 2024/1689 12.7.2024 ELI: http://data.europa.eu/eli/reg/2024/1689/oj 1/144(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) Position of the European Parliament of 13 March 2024 (not yet published in the Official Jour nal) and decision of the Council of May 2024. guarante eing the unif orm protect ion of overriding reasons of public interest and of rights of persons throughout the internal marke t on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the exte nt that this Regulation contains specif ic rules on the protect ion of individuals with regard to the processing of personal data concer ning restr ictions of the use of AI syste ms for remote biometr ic 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 biometr ic cate gorisation for the purpose of law enforcement, it is appropr iate to base this Regulation, in so far as those specific rules are concer ned, on Article 16 TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropr iate to consult the European Data Protection Board. (4) AI is a fast evolving family of technologies that contr ibut es to a wide array of economic, environmental and societal benefits across the entire spectr um of industr ies and social activities. By imp roving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key comp etitive advantages to under takings and suppor t socially and environmentally beneficial outcomes, for exam ple in healthcare, agriculture, food safety , education and training, media, spor ts, culture, infrastr ucture manag ement, energy , transpor t and logistics, public services, secur ity, justice, resource and energy efficiency , environmental monitoring, the conser vation and restoration of biodiversity and ecosystems and climate change mitig ation and adap tation. (5) 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 protect ed by Union law. Such harm might be material or immater ial, including physical, psychological, societal or economic harm. (6) Given the major impact that AI can have on society and the need to build trust, it is vital for AI and its regulator y framew ork to be developed in accordance with Union values as enshr ined in Article 2 of the Treaty on European Union (TEU), the fundamental rights and freedoms enshr ined in the Treaties and, pursuant to Article 6 TEU, the Char ter. As a prerequisite , AI should be a human-centr ic technology . It should serve as a tool for people, with the ultimate aim of increasing human well-being. (7) In order to ensure a consistent and high level of protection of public intere sts as regard s health, safety and fundamental rights, common rules for high-r isk AI syste ms should be established. Those rules should be consiste nt with the Char ter, non-discr iminat ory 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 trustw orthy AI of the High-Level Exper t Group on Artificial Intellig ence (AI HLEG). (8) A Union lega l framew ork laying down harmonised rules on AI is theref ore needed to foster the development, use and uptake of AI in the inter nal marke t that at the same time meets a high level of protect ion of public interests, such as health and safety and the prot ection of fundamental rights, including democracy , the rule of law and environmental protect ion as recognised and protect ed by Union law. To achieve that objective, rules regulating the placing on the marke t, the putting into service and the use of certain AI systems should be laid down, thus ensur ing the smooth functioning of the internal market and allowi ng those systems to benefit from the principle of free move ment of goods and services. Those rules should be clear and robust in protecting fundamental rights, suppor tive of new innovative solutions, enabling a European ecosyste m of public and private actor s creating AI syste ms in line with Union values and unlocking the potential of the digital transf ormation across all regions of the Union. By laying down those rules as well as measures in suppor t of inno vation with a particular focus on small and medium enterprises (SMEs), including startups, this Regulation suppor ts the objective of promoting the European human-centr ic approach to AI and being a global leader in the development of secure, trustwor thy and ethical AI as stated by the European Council (5), and it ensures the prot ection of ethical principles, as specific ally request ed by the European Parliament (6).

http://data.europa.eu/eli/reg/2024/1689/oj(5) European Council, Special meeting of the European Council (1 and 2 October 2020) — Conclusions, EUC O 13/20, 2020, p. 6. (6) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framew ork of ethical aspects of artificia l intellig ence, robotics and relat ed technologies, 2020/2012(INL). (9) Harmonised rules applicable to the placing on the mark et, the putting into service and the use of high-r isk AI syste ms 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 Framewo rk). The harmonised rules laid down in this 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 protect ion, consumer prot ection, fundamental rights, employment, and prot ection of work ers, and product safety , to which this Regulation is comp lementar y. As a consequence, all rights and remedies provid ed for by such Union law to consumers, and other persons on whom AI syste ms may have a nega tive impact, including as rega rds the comp ensation of possible damage s pursuant to Council Directive 85/374/EEC (10) remain unaff ected and fully applicable. Further more, in the context of employment and protect ion of workers, this Regulation should theref ore not affect Union law on social policy and national labour law, in compliance with Union law, concer ning emplo yment and working conditions, including health and safety at work and the relationship between emp loyers 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 specif ic industr ial relations syste ms in Member States as well as the right to negotiat e, 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 platf orm work laid down in a Directive of the European Parliament and of the Council on imp roving working conditions in platf orm work. Moreover , this Regulation aims to strengthen the effectiveness of such existing rights and remedies by establishing specific requirements and obliga tions, including in respect of the transparency , technical documentation and record-keepi ng of AI syste ms. Further more, the obliga tions placed on various operat ors involved in the AI value chain under this Regulation should apply without prejudice to national law, in com pliance 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 exam ple, national labour law and law on the protection of minors, namely persons below the age of 18, taking into account the UNCR C General Comment No 25 (2021) on children’s rights in relation to the digital environment, insofa r as they are not specif ic to AI syste ms and pursue other legitimate public interest objectives, should not be affected by this Regulation. (10) The fundamental right to the prot ection of personal data is safegua rded 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 prot ects private life and the confi dentiality 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 lega l 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 gover ning the processing of personal data, including the tasks and powers of the independent super visor y author ities compet ent to monito r compliance with those instr uments. It also does not affect the obliga tions of providers and deplo yers of AI syste ms in their role as data controllers or processors stemming from Union or national law on the prot ection of personal data in so far as the design, the development or the use of AI syste ms involves the processing of personal data. It is also appropr iate to clarify that data subjects continue to enjo y all the OJ L, 12.7.2024 EN ELI: http://data.europa.eu/eli/reg/2024/1689/oj 3/144(7) 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 L 218, 13.8.2008, p. 30). (8) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the mark eting of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82). (9) 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) Council Directive 85/374/EEC of 25 July 1985 on the appro ximation of the laws, regulations and administrative provisions of the Member States concer ning liability for defe ctive products (OJ L 210, 7.8.1985, p. 29). (11) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr il 2016 on the prot ection 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) 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) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr il 2016 on the prot ection of natural persons with regard to the processing of personal data by compet ent author ities for the purposes of the prevention, investig ation, 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) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concer ning the processing of personal data and the prot ection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37). rights and guarantees awarded to them by such Union law, including the rights related to solely automat ed individual decision-making, including prof iling. Harmonised rules for the placing on the marke t, the putting into service and the use of AI systems established under this Regulation should facilitate the effective imp lementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protect ion of personal data and of other fundamental rights. (11) This Regulation should be without prejudice to the provisions rega rding the liability of provider s of intermediar y services as set out in Regulation (EU) 2022/2065 of the European Parliament and of the Council (15). (12) 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 inter national conve rgence and wide accep tance, while providing the flexibility to accommodate the rapid technologi cal developments in this field. Moreo ver, the definition should be

based on key char acter istics of AI systems that distinguish it from simpler traditional software syste ms or programming approac hes and should not cover syste ms that are based on the rules defined solely by natural persons to auto matically execute operations. A key character istic of AI syste ms is their capability to infer . This capability to infer refers to the process of obtaining the outputs, such as predictions, cont ent, recommendations, or decisions, which can influence physica l and virtual envir onments, and to a capability of AI syste ms to derive models or algor ithms, or both, from inputs or data. The techniques that enable inference while building an AI syste m include machi ne learning approaches that learn from data how to achieve certain objectives, and logic- and kno wledge-based approac hes that infer from encoded knowle dge or symbolic representation of the task to be solved. The capacity of an AI syste m to infer transcends basic data processing by enabling learning, reasoning or modelling. The term ‘mach ine-based’ refers to the fact that AI systems run on machi nes. The reference to explicit or implicit objectives underscores that AI syste ms can operat e according to explicit defined objectives or to imp licit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific cont ext. For the purposes of this Regulation, envir onments should be understood to be the contexts in which the AI systems operate, whereas outputs generated by the AI syste m reflect diffe rent functions perfo rmed by AI syste ms and include predictions, cont ent, recommendations or decisions. AI syste ms are designed to operate with varying levels of autonom y, meaning that they have some degree of independence of actions from human involvement and of capabilities to operat e without human intervention. The adap tiveness that an AI syste m could exhibit after deplo yment, refers to self-lear ning capabilities, allowi ng the syste m to change while in use. AI syste ms can be used on a stand-alone basis or as a compo nent of a product, irrespective of whether the syste m is phys ically integrated into the product (embedded) or serves the functionality of the product without being integrat ed therein (non-embedded). (13) The notion of ‘deplo yer’ referred to in this Regulation should be interpreted as any natural or lega l person, including a public author ity, agency or other body , using an AI system under its author ity, excep t where the AI syste m is used in the course of a personal non-profess ional activity . Depending on the type of AI syste m, the use of the system may affect persons other than the deplo yer. (14) The notion of ‘biometr ic data’ used in this Regulation should be inter preted in light of the notion of biometr ic 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. Biometr ic data can allow for the authentication, identification or cate gorisation of natural persons and for the recognition of emotions of natural persons. (15) The notion of ‘biometr ic identifi cation’ referred to in this Regulation should be defined as the auto mated recognition of physical, physiological and behavi oural human features such as the face, eye move ment, body shape, voice, prosody , gait, posture, hear t rate, blood pressure, odour , keystrok es character istics, for the purpose of establishing an individual’s identity by compari ng biometr ic data of that individual to stored biometr ic data of individuals in a refere nce database, irrespective of whether the individual has given its consent or not. This excludes AI syste ms intended to be used for biometr ic verificati on, which includes authentication, whose sole purpose is to confi rm that a specific natural person is the person he or she claims to be and to confi rm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having secur ity access to premises.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Sing le Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1). (16) The notion of ‘biometr ic catego risation’ refer red to in this Regulation should be defined as assigning natural persons to specif ic cate gories on the basis of their biometr ic data. Such specif ic catego ries can relate to aspects such as sex, age, hair colour , eye colour , tattoos, behavio ural or personality traits, languag e, religion, membership of a national minor ity, sexual or political orientation. This does not include biometr ic catego risation systems that are a purely ancillar y 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 circum vent the applicability of the rules of this Regulation. For example, filters cate gorising facial or body features used on online marke tplaces could constitute such an ancillar y 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 displa y of the product on him or herself and help the consumer to mak e a purcha se decision. Filte rs used on online social netw ork services which cate gorise facial or body features to allow users to add or modify pictures or videos could also be considered to be ancillar y feature as such filter cannot be used without the principal service of the social netw ork services consisting in the shar ing of cont ent online. (17) The notion of ‘remot e biometr ic identifica tion syste m’ referred to in this Regulation should be defined functionally , as an AI syste m intended for the identifica tion of natural persons without their active involvement, typically at a distance, through the comp arison of a person’s biometr ic data with the biometr ic data contained in a reference database, irrespectively of the particular technology , processes or types of biometr ic data used. Such remote biometr ic identifica tion systems are typically used to perceive multiple persons or their behavio ur simultaneously in order to facilitate signif icantly the identification of natural persons without their active involvement. This excludes AI syste ms intended to be used for biometr ic verification, which includes authentication, the sole purpose of which is to confi rm that a specif ic natural person is the person he or she claims to be and to confi rm the identity of a natural person for the sole purpose of having access to a service, unloc king a device or having secur ity access to premises. That exclusion is justified by the fact that such syste ms are likely to have a minor imp act on fundamental rights of natural persons comp ared to the remote biometr ic identifi cation syste ms which may be used for the processing of the biometr ic data of a large number of persons without their active involvement. In the case of ‘real-time’ syste ms, the captu ring of the biometr ic data, the comp arison and the identifi cation occur all instantaneously , near -instantaneously or in any event without a significant dela y. In this regard, there should be no scope for circum venting the rules of this Regulation on the ‘real-time’ use of the AI systems concer ned by providing for minor dela ys. ‘Real-time’ syste ms involve the use of ‘live’ or ‘near -live’ material, such as video footage , generat ed by a camera or other device with similar functionality . In the case of ‘post’ systems, in contrast, the biometr ic data has already been captured and the comp arison and identifica tion occur only after a significant dela y. This involves mat erial, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the syste m in respect of the natural persons concer ned. (18) The notion of ‘emotion recognition system’ referred to in this Regulation should be defined as an AI syste m for the purpose of identifying or inferr ing emotions or

intentions of natural persons on the basis of their biometr ic data. The notion refers to emotions or intent ions such as happiness, sadness, anger , surprise, disgust, embar rassment, excitement, shame, contem pt, satisfaction and amusement. It does not include physical states, such as pain or fatigue, including, for exam ple, syste ms used in detecting the state of fatigue of profe ssional 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 inferr ing emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the moveme nt of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whisper ing. (19) For the purposes of this Regulation the notion of 'publicly accessible space' should be understood as referring to any phys ical space that is accessible to an undeter mined 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 exam ple, shops, restaurants, cafés; for services, for exam ple, banks, professional activities, hospitality ; for spor t, for exam ple, swimming pools, gyms, stadiums; for transpor t, for exam ple, bus, metro and railwa y stations, airports, means of transpor t; for entertainment, for exam ple, cinemas, theatres, museums, concer t and confe rence halls; or for leisure or other wise, for example, public roads and squares, park s, forests, playgrounds. A space should also be classified as being publicly accessible if, regard less of pote ntial capacity or secur ity restr ictions, access is subject to certain predete rmined conditions which can be fulfilled by an undeter mined number of persons, such as the purc hase of a ticket or title of transpor t, prior registration or having a certain age. In contrast, a space should not be considered to be publicly accessible if access is limited to specif ic and defined natural persons through either Union or national law directly related to public safety or secur ity or through the clear manif estation OJ L, 12.7.2024 EN ELI: http://data.europa.eu/eli/reg/2024/1689/oj 5/144 of will by the person having the relevant author ity over the space. The factual possibility of access alone, such as an unloc ked door or an open gate in a fence, does not imp ly that the space is publicly accessible in the presence of indications or circumstances suggesting the contrar y, such as. signs prohibiting or restr icting access. Compan y and factory premises, as well as offices and workplaces that are intende d to be accessed only by relevant emp loyees and service providers, are spaces that are not publicly accessible. Publicly accessible spaces should not include prisons or border control. Some other spaces may compr ise both publicly accessible and non-publicly accessible spaces, such as the hallwa y of a private residential building necessar y to access a docto r'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 howe ver be determined on a case-by-c ase basis, having regard to the specif icities of the individual situation at hand. (20) In order to obtain the great est benefits from AI syste ms while prot ecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deplo yers and affect ed persons with the necessar y notions to mak e informed decisions regarding AI systems. Those notions may vary with regard to the relevant cont ext 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 inter pret the AI system's output, and, in the case of affected persons, the kno wledge necessar y to understand how decisions taken with the assistance of AI will have an imp act 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 appropr iate compliance and its correct enforcement. Further more, the wide implementation of AI literac y measures and the introduction of appropr iate follow-up actions could contr ibut e to impro ving work ing conditions and ultimately sustain the consolidation, and inno vation path of trustwor thy AI in the Union. The European Artificial Intellig ence Board (the 'Board') should suppor t the Commission, to promot e AI litera cy tools, public awareness and understanding of the benefits, risks, safegua rds, rights and obliga tions in relation to the use of AI syste ms. In cooperation with the relevant stak eholders, the Commission and the Member States should facilitate the drawing up of voluntar y codes of conduct to advance AI literacy among persons dealing with the development, operation and use of AI. (21) In order to ensure a level playing field and an effective protect ion of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to provid ers of AI syste ms in a non-discr iminat ory manner , irrespective of whether they are established within the Union or in a third countr y, and to deplo yers of AI syste ms established within the Union. (22) In light of their digital nature, certain AI syste ms should fall within the scope of this Regulation even when they are not placed on the marke t, 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 countr y in relation to an activity to be perform ed by an AI system that would qualify as high-r isk. In those circumstances, the AI syste m used in a third countr y by the operator could process data lawfully collected in and transferre d from the Union, and provide to the contracting operato r in the Union the output of that AI system resulting from that processing, without that AI syste m being placed on the marke t, put into service or used in the Union. To prevent the circum vention of this Regulation and to ensure an effective prot ection of natural persons located in the Union, this Regulation should also apply to providers and deplo yers of AI systems that are established in a third countr y, to the exte nt the output produced by those syste ms is intende d to be used in the Union. Nonetheless, to take into account existing arrang ements and special needs for future cooperation with foreign partners with whom information and evidence is exchang ed, this Regulation should not apply to public author ities of a third countr y and inter national organisations when acting in the framework of cooperation or inter national 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 countr y or international organisation provides adequate safegua rds with respect to the prot ection of fundamental rights and freedoms of individuals. Where relevant, this may cover activities of entities entr usted by the third countr ies to carry out specif ic tasks in suppor t of such law enforcement and judicial cooperation. Such framew ork for cooperation or agreements have been established bilat erally between Member States and third countr ies or between the European Union, Europol and other Union agencies and third countr ies and international organisations. The author ities compet ent for super vision of the law enforcement and judicial author ities under this Regulation should assess whether those framew orks for cooperation or inter national agreements include adequate safeguards with respect to the protect ion of fundamental rights and freedoms of individuals. Recipient national EN OJ L, 12.7.2024 6/144 ELI: http://data.europa.eu/eli/reg/2024/1689/oj author ities and Union institutions, bodies, offices and agencies making use of such outputs in the Union remain accountable to ensure their use comp lies with Union law. When those inter national 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) This Regulation should also apply to Union institutions, bodies, offices and agencies when acting as a provid er or deplo yer of an AI syste m. (24) If, and insofa r as, AI systems are placed on the marke t, put into service, or used with or without modification of such syste ms for militar y, defe nce or national secur ity purposes, those should be excluded from the scope of this Regulation regard less of which type of entity is carrying out those activities, such as whether it is a public or private entity . As regard s militar y and defe nce purposes, such exclusion is justif ied both by Article 4(2) TEU and by the specificities of the Member States' and the common Union defence policy covered by Chapt er 2 of Title V TEU that are subject to public inter national law, which is theref ore the more appropr iate legal framew ork for the regulation of AI systems in the cont ext of the use of lethal force and other AI syste ms in the context of militar y and defence activities. As rega rds national secur ity purposes, the exclusion is justified both by the fact that national secur ity remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specif ic nature and operational needs of national secur ity activities and specific national rules applicable to those activities. Nonetheless, if an AI system developed, placed on the marke t, put into service or used for militar y, defence or national secur ity purposes is used outside those temporar ily or permanently for other purposes, for exam ple, civilian or humanitar ian purposes, law enforcement or public secur ity purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the AI syste m for other than militar y, defe nce or national secur ity purposes should ensure the compliance of the AI syste m with this Regulation, unless the syste m is already compliant with this Regulation. AI syste ms placed on the marke t or put into service for an excluded purpose, namely militar y, defe nce or national secur ity, and one or more non-exclu ded 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 secur ity, defence and militar y activities, rega rdless of the type of entity carrying out those activities, to use AI systems for national secur ity, militar y and defe nce purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the marke t for civilian or law enforcement purposes which is used with or without modifi cation for militar y, defence or national secur ity purposes should not fall within the scope of this Regulation, rega rdless of the type of entity carrying out those activities. (25) This Regulation should suppor t inno vation, should respect freedom of science, and should not under mine research and development activity . It is theref ore necessar y to exclude from its scope AI syste ms and models specifically developed and put into service for the sole purpose of scientifi c research and development. Moreove r, it is necessar y to ensure that this Regulation does not other wise affect scientific research and development activity on AI syste ms or models prior to being placed on the market or put into service. As regards product-or iented research, testing and development activity rega rding AI syste ms or models, the provisions of this Regulation should also not apply prior to those syste ms and models being put into service or placed on the marke t. That exclusion is without prejudice to the obligation to comp ly with this Regulation where an AI system falling into the scope of this Regulation is placed on the marke t or put into service as a result of such research and development activity and to the application of provisions on AI regulato ry sandbo xes and testing in real world conditions. Further more, without

prejudice to the exclusion of AI syste ms specif ically developed and put into service for the sole purpose of scientifi c researc h 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 profe ssional standards for scientific research and should be conducte d in accordance with applicable Union law. (26) In order to introduce a propor tionate and effective set of binding rules for AI syste ms, a clearly defined risk-based approac h should be follo wed. That approac h should tailor the type and content of such rules to the intensity and scope of the risks that AI syste ms can generate. It is theref ore necessar y to prohibit certain unaccept able AI practices, to lay down requirements for high-r isk AI systems and obligati ons for the relevant operators, and to lay down transparency obligations for certain AI syste ms.OJ L, 12.7.2024 EN ELI: http://data.europa.eu/eli/reg/2024/1689/oj 7/144 (27) While the risk-based approac h is the basis for a propor tionate and effective set of binding rules, it is imp ortant to recall the 2019 Ethics guidelines for trustwo rthy AI developed by the independent AI HLEG appoint ed 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 trustwor thy and ethically sound. The seven principles include human agency and oversight ; technical robustness and safety; privacy and data gover nance; transparency ; diversity , non-discr imination and fairness; societal and envir onmental well-being and accountability . Without prejudice to the legally binding requirements of this Regulation and any other applicable Union law, those guidelines contr ibut e to the design of coherent, trustwor thy and human-centr ic AI, in line with the Char ter and with the values on which the Union is founded. According to the guidelines of the AI HLEG, human agency and oversight means that AI systems are developed and used as a tool that serves people, respects human dignity and personal autonom y, and that is functioning in a way that can be appropr iately controlled and overseen by humans. Technical robustness and safety means that AI syste ms are developed and used in a way that allows robustness in the case of problems and resilience against attempts to alter the use or perform ance of the AI syste m so as to allow unla wful use by third parties, and minimise uninte nded harm. Privacy and data gove rnance means that AI syste ms are developed and used in accordance with privacy and data prot ection rules, while processing data that meets high standards in terms of quality and integrity. Transparency means that AI syste ms are developed and used in a way that allows appropr iate traceability and explainability , while making humans aware that they communicate or interact with an AI syste m, as well as duly informing deplo yers of the capabilities and limitations of that AI system and affected persons about their rights. Diversity , non-discr imination and fairne ss means that AI syste ms are developed and used in a way that includes diverse actor s and promotes equal access, gender equality and cultural diversity , while avoiding discr iminatory imp acts and unfa ir biases that are prohibite d by Union or national law. Social and envir onmental well-being means that AI systems are developed and used in a sustainable and environmentally friendly manner as well as in a way to benefi t all human beings, while monitori ng and assessing the long-term imp acts on the individual, society and democracy . The application of those principles should be translat ed, when possible, in the design and use of AI models. They should in any case serve as a basis for the draf ting of codes of conduct under this Regulation. All stakeholders, including industr y, academia, civil society and standardisation organisations, are encourag ed to take into account, as appropr iate, the ethical principles for the development of voluntary best

practices and standards. (28) 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 prohibite d because they contradict Union values of respect for human dignity , freedom, equality , democracy and the rule of law and fundamental rights enshr ined in the Char ter, including the right to non-discr imination, to data prot ection and to privacy and the rights of the child. (29) AI-enabled manipulative techniques can be used to persuade persons to engage in unwant ed behaviours, or to deceive them by nudging them into decisions in a way that subver ts and imp airs their autonom y, decision-making and free choices. The placing on the marke t, the putting into service or the use of certain AI syste ms with the objective to or the effect of mat erially distor ting human behavio ur, whereb y signifi cant harms, in particular having sufficiently imp ortant adverse impacts on phys ical, psychological health or financ ial intere sts are likely to occur , are particularly dangerous and should theref ore be prohibite d. Such AI syste ms deplo y subliminal comp onents such as audio, image, video stimuli that persons cannot perceive, as those stimuli are beyond human percep tion, or other manipulative or decept ive techniques that subver t or imp air person's auto nomy , 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, insofa r as they may materially distor t their behavio ur in a significantly harmful manner . In addition, AI syste ms may also other wise exploit the vulnerabilities of a person or a specif ic 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 mak e those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minor ities. Such AI syste ms can be placed on the marke t, put into service or used with the objective to or the effect of materially distor ting the behavi our of a person and in a manner that causes or is reasonably likely to cause signifi cant harm to that or another person or groups of persons, including harms that may be accumulated over time and should theref ore be prohibite d. It may not be possible to assume that there is an EN OJ L, 12.7.2024 8/144 ELI: http://data.europa.eu/eli/reg/2024/1689/oj(16) Directive (EU) 2019/882 of the European Parliament and of the Council of 17 Apr il 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70). intention to distor t behavio ur where the distor tion results from factors exter nal to the AI syste m which are outside the control of the provid er or the deplo yer, namely factors that may not be reasonably foreseeable and theref ore not possible for the provider or the deplo yer of the AI syste m to mitigat e. In any case, it is not necessar y for the provid er or the deplo yer to have the intention to cause signifi cant harm, provided that such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices are complement ary to the provisions contained in Directive 2005/29/EC of the European Parliame nt and of the Council (17), in particular unfa ir 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 other wise. The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychologi cal treatment of a mental disease or phys ical rehabilitation, when those practices are

carried out in accordance with the applicable law and medical standards, for exam ple explicit consent of the individuals or their legal representatives. In addition, common and legitimate commercial practices, for example in the field of adver tising, that comply with the applicable law should not, in themselves, be rega rded as constituting harmful manipulative AI-enabled practices. (30) Biometr ic categor isation syste ms that are based on natural persons' biometr ic data, such as an individual person's face or finger print, to deduce or infer an individuals ' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation should be prohibite d. That prohibition should not cover the lawful labelling, filter ing or categori sation of biometr ic data sets acquired in line with Union or national law according to biometr ic data, such as the sorting of imag es according to hair colour or eye colour , which can for exam ple be used in the area of law enforcement. (31) AI systems provid ing social scor ing of natural persons by public or private actors may lead to discr iminat ory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discr imination and the values of equality and justice. Such AI syste ms evaluate or classify natural persons or groups thereof on the basis of multiple data points related to their social behavio ur in multiple contexts or known, inferred or predicted personal or personality character istics over certain periods of time. The social score obtained from such AI systems may lead to the detr imental or unfa vourable treatment of natural persons or whole groups thereof in social cont exts, which are unrelate d to the context in which the data was originally generat ed or collect ed or to a detr imental treatment that is dispropor tionate or unjustifie d to the gravity of their social behavio ur. AI systems entailing such unaccept able scor ing practices and leading to such detr imental or unfa vourable outcomes should theref ore 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) The use of AI syste ms for 'real-time' remote biometr ic identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concer ned persons, to the extent that it may affect the private life of a large part of the population, evok e a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI syste ms intende d for the remote biometr ic identifi cation of natural persons can lead to biased results and entail discr iminatory effects. Such possible biased results and discr iminatory effects are particularly relevant with regard to age, ethnicity , race, sex or disabilities. In addition, the immediacy of the impact and the limited oppor tunities for further chec ks or corrections in relation to the use of such systems operating in real-time carry height ened risks for the rights and freedoms of the persons concer ned in the cont ext of, or impacted by, law enforcement activities. (33) The use of those systems for the purpose of law enforcement should theref ore be prohibited, except in exhaustively listed and narrowly defined situations, where the use is strictly necessar y 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 phys ical safety of natural persons or of a terrorist attac k; and the localisation or identification of perpetrat ors or suspects of the criminal offences listed in an annex to this Regulation, where those criminal offences are punishable in the Member State concer ned by a custo dial sentence or a detention OJ L, 12.7.2024 EN ELI: http://data.europa.eu/eli/reg/2024/1689/oj 9/144(17) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concer ning unfair

business-to-consumer commercial practices in the inter nal 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 ('Unf air Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22). 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 custo dial sent ence or detention order in accordance with national law contr ibut es to ensur ing that the offence should be serious enough to potentially justify the use of 'real-time' remot e biometr ic identification syste ms. 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, likel y to be more relevant than others, in that the recourse to 'real-time' remote biometr ic identification could, foreseeably , be necessar y and propor tionate to highly varying degrees for the practical pursuit of the localisation or identification of a perpetrat or or suspect of the different criminal offences listed and having rega rd to the likely differences in the seriousness, probability and scale of the harm or possible negati ve consequences. An imminent threat to life or the physical safety of natural persons could also result from a serious disruption of critical infrastr ucture, 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 destr uction of such critical infrastr ucture 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 preser ve the ability for law enforcement, border control, immigration or asylum author ities to carry out identity checks in the presence of the person concer ned in accordance with the conditions set out in Union and national law for such chec ks. In particular , law enforcement, border control, immigration or asylum author ities should be able to use information syste ms, in accordance with Union or national law, to identify persons who, 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 author isation. This could be, for exam ple, 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 author ities. (34) In order to ensure that those syste ms are used in a responsible and propor tionate manner , it is also impor tant to establish that, in each of those exhaustively listed and narrowly defined situations, certain elements should be take n 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 concer ned and the safeguards and conditions provid ed for with the use. In addition, the use of 'real-time' remot e biometr ic identifi cation systems in publicly accessible spaces for the purpose of law enforcement should be deplo yed only to confir m the specif ically targe ted individual's identity and should be limit ed to what is strictly necessar y concer ning the period of time, as well as the geographic and personal scope, having rega rd in particular to the evidence or indications rega rding the threats, the victims or perpetrat or. The use of the real-time remote biometr ic identifica tion system in publicly accessible spaces should be author ised only if the relevant law enforcement author ity has comp leted a fundamental rights impact assessment and, unless provid ed other wise in this Regulation, has register ed the syste m in the database as set out in this Regulation. The reference database of persons should be appropr iate for each use case in each of the situations

mentioned above. (35) Each use of a ‘real-time’ remote biometr ic identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specif ic author isation by a judicial author ity or by an independent administrative author ity of a Member State whose decision is binding. Such author isation 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 justifi ed situations on grounds of urgency , namely in situations where the need to use the syste ms concer ned is such as to mak e it effectively and objectively impossible to obtain an author isation before commencing the use of the AI system. In such situations of urgency , the use of the AI syste m should be restr icted to the absolute minimum necessar y and should be subject to appropr iate safeguards and conditions, as determined in national law and specif ied in the cont ext of each individual urgent use case by the law enforcement author ity itself. In addition, the law enforcement author ity should in such situations request such author isation while provid ing the reasons for not having been able to request it earlier , without undue dela y and at the latest within 24 hours. If such an author isation is rejected, the use of real-time biometr ic identification systems linked to that author isation should cease with immediate effect and all the data related to such use should be discarded and delete d. Such data includes EN OJ L, 12.7.2024 10/144 ELI: http://data.europa.eu/eli/reg/2024/1689/oj(18) 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). (19) 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 (OJ L 333, 27.12.2022, p. 164). input data directly acquired by an AI syste m in the course of the use of such system as well as the results and outputs of the use linked to that author isation. It should not include input that is lega lly acquired in accordance with another Union or national law. In any case, no decision producing an adverse lega l effect on a person should be taken based solely on the output of the remot e biometr ic identification system. (36) 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 marke t surveillance author ity and the national data prot ection author ity should be notif ied of each use of the real-time biometr ic identification system. Market surveillance author ities and the national data prot ection author ities that have been notif ied should submit to the Commission an annual repor t on the use of real-time biometr ic identifi cation syste ms. (37) Further more, it is appropr iate to provid e, 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 concer ned has decided to expressly provide for the possibility to author ise 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 provid e for such a possibility in respect of some of the objectives capable of justifying author ised use identified in this Regulation. Such national rules should be notified to the Commission within 30 days of their adop tion. (38) The use of AI syste ms for real-time remote biometr ic identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessar ily involves the processing of biometr ic 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 biometr ic data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometr ic data

involved in an exhaustive manner . Theref ore, 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 comp etent author ities, where they act for purpose of law enforcement, to use such syste ms and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In that cont ext, 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 biometr ic identifica tion syste ms in publicly accessible spaces for purposes other than law enforcement, including by com petent author ities, should not be covered by the specif ic framew ork regard ing such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should theref ore not be subject to the requirement of an author isation under this Regulation and the applicable detailed rules of national law that may give effect to that author isation. (39) Any processing of biometr ic data and other personal data involved in the use of AI syste ms for biometr ic identification, other than in connection to the use of real-time remote biometr ic identification syste ms 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 biometr ic data subject to limit ed exceptions as provided in those Articles. In the application of Article 9(1) of Regulation (EU) 2016/679, the use of remot e biometr ic identifi cation for purposes other than law enforcement has already been subject to prohibition decisions by national data protection author ities. (40) 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, secur ity and justice, as annexe d 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 exte nt it applies to the use of biometr ic categor isation syste ms for activities in the field of police cooperation and judicial cooperation in criminal matt ers, Article 5(1), first subparagraph, point (d), to the exte nt it applies to the use of AI syste ms covered by that provision, Article 5(1), first subparagraph, point (h), Article 5(2) to (6) and Article 26(10) of this Regulation adop ted 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 Chapt er 4 or Chapt er 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules gover ning the forms of judicial cooperation in criminal matt ers or police cooperation which require com pliance with the provisions laid down on the basis of Article 16 TFEU. (41) In accordance with Articles 2 and 2a of Proto col No 22 on the position of Denmark, annexe d 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 exte nt it applies to the use of biometr ic categor isation syste ms for activities in the field of police cooperation and judicial cooperation in criminal matt ers, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI syste ms covered by that provision, Article 5(1), first subparagraph, point (h), (2) to (6) and Article 26(10) of this Regulation OJ L, 12.7.2024 EN ELI: http://data.europa.eu/eli/reg/2024/1689/oj 11/144 adop ted 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 Chap ter 4 or Chapt er 5 of Title V of Part Three of the TFEU. (42) In line with the presump tion of innocence, natural persons in the Union

should alwa ys be judged on their actual behavi our. Natural persons should never be judg ed on AI-predicted behavio ur based solely on their prof iling, personality traits or char acter istics, 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. Theref ore, risk assessments carried out with rega rd to natural persons in order to assess the likelihood of their offending or to predict the occur rence of an actual or pote ntial criminal offence based solely on prof iling them or on assessing their personality traits and character istics should be prohibited. In any case, that prohibition does not refer to or touch upon risk analytics that are not based on the profil ing of individuals or on the personality traits and charact eristics of individuals, such as AI systems using risk analytics to assess the likelihood of financ ial fraud by under takings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs author ities, for exam ple on the basis of known traff icking routes. (43) The placing on the mark et, the putting into service for that specific purpose, or the use of AI syste ms that create or expand facial recognition databases through the untarg eted scraping of facial images from the inter net or CCT V footage, should be prohibite d 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) There are serious concer ns 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 sing le individual. Among the key shor tcomings of such syste ms are the limited reliability , the lack of specificity and the limit ed generalisability . Theref ore, AI systems identifying or inferr ing emotions or intentions of natural persons on the basis of their biometr ic data may lead to discr iminat ory outcomes and can be intrusive to the rights and freedoms of the concer ned persons. Consider ing the imbalance of power in the cont ext of work or education, combined with the intrusive nature of these syste ms, such systems could lead to detr imental or unfa vourable treatment of certain natural persons or whole groups thereof. Theref ore, the placing on the marke t, the putting into service, or the use of AI syste ms intended to be used to detect the emotional state of individuals in situations related to the workplace and education should be prohibite d. That prohibition should not cover AI systems placed on the mark et strictly for medical or safety reasons, such as systems intended for therapeutical use. (45) Practices that are prohibited by Union law, including data prot ection law, non-discr imination law, consumer prot ection law, and competition law, should not be affected by this Regulation. (46) High-r isk AI systems should only be placed on the Union marke t, put into service or used if they comply with certain mandato ry requirements. Those requirements should ensure that high-r isk AI systems available in the Union or whose output is other wise used in the Union do not pose unaccepta ble risks to important Union public interests as recognised and protect ed by Union law. On the basis of the New Legislative Framework, as clarified in the Commission notice ‘The “Blue Guide” on the imp lementation of EU product rules 2022’ (20), the general rule is that more than one lega l 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 availa ble or putting into service can take EN OJ L, 12.7.2024 12/144 ELI: http://data.europa.eu/eli/reg/2024/1689/oj(20) OJ C 247, 29.6.2022, p. 1. (21) Regulation

(EU) 2017/745 of the European Parliament and of the Council of 5 Apr il 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) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 Apr il 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) Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machiner y, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24). place only when the product comp lies with all applicable Union harmonisation legislation. To ensure consiste ncy and avoid unnecessar y administrative burdens or costs, provid ers of a product that contains one or more high-r isk AI syste ms, 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 com pliance of a product that contains one or more AI syste ms with all applicable requirements of the Union harmonisation legislation in an optima l manner . AI syste ms identified as high-r isk should be limit ed 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 pote ntial restr iction to international trade. (47) AI syste ms could have an adverse impact on the health and safety of persons, in particular when such syste ms operat e as safety comp onents of products. Consiste nt with the objectives of Union harmonisation legislation to facilitate the free move ment of products in the inter nal market and to ensure that only safe and other wise comp liant products find their way into the market, it is imp ortant that the safety risks that may be generated by a product as a whole due to its digital com ponents, including AI syste ms, are duly prevented and mitigat ed. For instance, increasing ly autono mous robots, whether in the cont ext of manuf actur ing or personal assistance and care should be able to safely operate and perfo rms their functions in complex environments. Similarly , in the health secto r where the stakes for life and health are particularly high, increasing ly sophisticat ed diagnostics systems and syste ms suppor ting human decisions should be reliable and accurate. (48) The extent of the adverse imp act caused by the AI syste m on the fundamental rights protect ed by the Char ter is of particular relevance when classifying an AI syste m 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-discr imination, the right to education, consumer protection, work ers' rights, the rights of persons with disabilities, gender equality , intellectual proper ty rights, the right to an effective remedy and to a fair trial, the right of defence and the presump tion of innocence, and the right to good administration. In addition to those rights, it is impor tant to highlight the fact that children have specif ic rights as enshr ined in Article 24 of the Char ter and in the Unit ed Nations Convention on the Rights of the Child, further developed in the UNCR C General Comment No 25 as regard s the digital environment, both of which require consideration of the children's