Council of the European Union
General Secretariat

Brussels, 20 September 2022

WK 12308/2022 INIT

LIMITE

TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Artificial Intelligence Act - DE Non-Paper on Separate Regulation of AI Systems for Public Administration

Delegations will find in the Annex the DE Non-Paper on Separate Regulation of AI Systems for Public Administration.

Regulation of AI – taking greater account of the specific characteristics of the public administration, particularly in the fields of security and migration

Germany is in favour of the regulation of AI systems and supports the European AI Act. This also includes the rapid, simultaneous regulation of AI systems for the public administration, in particular the security, migration and asylum authorities, and the tax and customs administration (including the Financial Intelligence Unit, FIU).

However, the particular requirements of the activities of the abovementioned authorities are not sufficiently taken into account in all respects by the current proposal. This is because it is difficult to fully reflect the specific interests of these authorities, along with the requirements in terms of fundamental rights that apply to public authority activities, within the primarily private law, internal market-focused rules in the proposed AI Act. It must be possible to carry out government functions while at the same time observing the direct commitment of the government administration to protect fundamental rights. The range of necessary individual exceptions / amendments in the individual provisions of the current draft regulation will lead to a lack of legal certainty for the addressees of the norms in question.

Germany is of the opinion that the specific characteristics of the public administration (and in particular those of the security, migration and asylum authorities, as well as the tax and customs authorities, including the FIU) can be better accommodated in a separate, specific technology act or in a separate section in the Regulation (referred to in this document as “separate regulation”). The provisions in the separate regulation should be exhaustive.

Regardless of Germany’s proposals for special regulations for other areas of the public administration, in accordance with the objectives of the draft regulation, this paper will put forward the following key points for security, migration and asylum authorities, and the tax and customs administration (including the FIU). Notwithstanding the potential need to amend the underlying regulatory architecture for the authorities listed, alongside general comments on potentially necessary amendments, Germany’s position is also stated on individual articles so that specific needs can be illustrated with concrete examples. Discussions are still under way in Germany regarding a range of points in the separate regulation; these discussions will be outlined in this paper. Germany therefore reserves the right to submit further comments.

1. Special characteristics of the field of law enforcement

The proposal from the Commission already lays down special regulations for the field of law enforcement. On the one hand, the special regulations aim to take into account the requirements in terms of fundamental rights for this particularly invasive area of the public

administration; see for example the prohibition in Article 5 (1) letter (d) of the proposal and the high-risk classification in Annex III no. 6 of the proposal. On the other, the proposal from the Commission includes special regulations aiming to ensure that law enforcement authorities can carry out their functions, for example Article 70 (2) of the proposal.

The current proposal from the Presidency of the Council of the EU contains further provisions of a similar nature, for example Article 47 (1a) of the proposal.

From Germany's point of view, the AI Act should be amended and supplemented with the following additional points, in order on the one hand to take into account particular threats to fundamental rights and on the other to ensure that government functions can be carried out.

a) Extension of the prohibition in Article 5 (1) letter (d) of the proposal

Remote real-time biometric identification in public spaces through AI must be ruled out by European law. However, retrograde biometric identification, e.g. during the evaluation of evidence, must not be ruled out by European law. However, discussions are still under way in regard to the prohibition in Article 5 (1) letter (d) of remote biometric identification systems. We reserve the right to submit further comments.

b) Achieving a balance between transparency and sufficient protection of confidential information in the field of law enforcement

Transparency is a key element of the protection strategy developed by the Commission in the AI Regulation and, in view of the legislative objective of creating trustworthy AI applications, it is generally to be welcomed.

In the field of law enforcement, the government may have opposing interests. This is because the success of the use of AI on the basis of government authority to do so may be put at risk by publishing the details and the functioning of AI apps deployed by law enforcement. The existing transparency provisions in the AI Regulation should therefore be examined in terms of whether and, if applicable, to what extent exceptions from the transparency obligations may be prudent, if and to the extent that these seem necessary and proportionate in individual cases due to conflicting security interests that are worthy of protection. However, potential conflicts between transparency and security need not lead only to negative exceptions to transparency obligations; they can also be resolved by implementing positive confidentiality requirements or adjustments regarding the bodies subject to the obligations in the Regulation. In this context, it is also necessary to examine whether additional provisions regarding confidentiality and data protection are required that could be addressed in a separate regulation. For example, the AI Regulation provides few concrete confidentiality requirements, for example in Article 70 (2), and even then, these only

apply to situations in which law enforcement authorities themselves are the developers or providers of AI applications.

This affects the following circumstances and provisions:

- **Non-publication of "notified bodies" in the field of law enforcement (see Article 35 (2) of the AI Regulation)**
  The German Federal Government is concerned that the publication of the list of "notified bodies" under Article 35 (2) of the AI Regulation, if it were to include bodies in the field of law enforcement, could facilitate illegal influence or scrutiny of such agencies, for example by foreign services. Do the Commission or the other Member States share this assessment? Should an exception be included in this regard enabling the Member State in question under certain conditions, which must first be defined in more detail, to refrain in individual cases from publishing law enforcement authorities in the list of notified bodies where security interests are at odds with this? German security authorities are in favour of this.

- **Non-publication of high-risk AI applications in the field of law enforcement (see Articles 60 and 61 of the AI Regulation)**
  The German Federal Government is concerned that public access to the EU database of high-risk AI applications provided for in Article 60 (5) of the AI Regulation could clash with justified security interests of the Member States. There are fears that even the publication of all AI applications that are operated or under development by the security authorities would make it easier to gain an overall picture of the operational capabilities of the authorities in question. Using this database, potential gaps in capabilities could be identified, or profiles of the focus areas of individual countries could be compiled. This could represent a security risk in itself and could impact the capabilities of the authorities. Do the Commission or the other Member States share this assessment? Should an exception be included in this regard in Articles 60 and 61 enabling the Member State in question under certain conditions, which must first be defined in more detail, to refrain in individual cases from publishing AI applications where security interests are at odds with this? German security authorities are in favour of this.

- **Agreement prior to transmitting confidential information (Article 70 (2) of the AI Regulation)**
  The Commission Proposal already stipulates that, prior to disclosing the confidential information listed in the provision, the national competent authority is to be consulted when such disclosure would jeopardise public and national security interests. Germany's view is that in the situations described, consultation alone is not sufficient.

Rather, when the conditions listed arise, the approval of the authority in question should be sought.

*"[…] shall not be disclosed without the prior ~~consultation~~ **approval […]**"*

- **Guaranteeing the confidentiality requirements of the security authorities within Article 16 of the AI Regulation**

  Discussions are under way in Germany of whether further requirements are necessary in Article 16 to protect confidentiality interests in those cases where high-risk AI systems from a (private) provider are deployed in law enforcement. Any further requirements should aim to balance potential conflicts of interest between the legislative objective of Article 16 and security needs as carefully as possible, for example by amending the bodies subject to the obligations in the Regulation. Specifically, a potential solution may be for the information required under Article 16 of the AI Regulation not to be transmitted to the national authority by the (private) provider, but by the user of the AI system. Discussion is currently under way in Germany of how the transmission of particularly sensitive data might take place. If, for example, the AI system of a (private) provider is used in another MS for security-relevant measures, it could be problematic from a security perspective if the (private) provider in such cases makes entirely public the way in which the AI system is specifically used. Risk management by the (private) provider during the lifecycle of the AI system could therefore be in conflict with State security interests (see Article 16 (a) in conjunction with Article 9 (2) and (3) of the proposal). For reasons of confidentiality and protection of methods, Germany is also critical of providers keeping technical documentation up to date in accordance with Article 11 (1) in cases where the AI system is used in the field of law enforcement. Would a possible solution in this area also be transferring certain obligations under Article 16 from the provider to the user, if and to the extent that State security interests require this? Do the Commission or the other Member States also consider this a relevant question?

- **Security requirements for examination and supervisory organisations in the field of law enforcement**

  Discussions are under way in Germany regarding the extent to which provisions should be put in place for adapted structures and competences for specific processes within the regulation of AI applications in the field of law enforcement, particularly for bodies carrying out examination and certification tasks in these areas, and whether the addressees of the associated disclosure obligations should be limited. Alongside general security matters, this could include, for example, any necessary regulations in

connection with tender processes and provisions regarding compliance with specific minimum standards and IT security procedures within the conformity process, in order to ensure a comprehensive evaluation that protects fundamental rights while providing sufficient IT security. Provisions could also be put in place for training requirements for staff of supervisory authorities (incl. provisions on security clearances and personnel security). The relevant provisions could be included in the separate regulation, or alternatively in additional articles of the AI Regulation. How do the Commission and the other Member States judge the need for relevant Europe-wide provisions to strengthen a uniform standard of protection?

c) Adaptation and differentiation in classification as high-risk AI (Annex III)

The categorisation proposed by the Commission of specific AI systems deployed by the security authorities as high risk in accordance with Annex III point 6 of the proposal was already discussed in detail during the Council negotiations. The presidency has already proposed amendments in this regard which are still under discussion among the Member States. The following points are currently under discussion in Germany:

- Letter (d): We request further clarification. The description of AI systems covered by letter (d) should be clear-cut. It must be ensured that systems without risk to health, safety or fundamental rights are not covered. For Germany, it is very important that letter (d) is defined more narrowly in this respect. At the same time, systems that pose a risk to the abovementioned protected interests must remain covered.
- Letter (f): Discussions are under way in Germany of whether the definition under Article 3 (4) of Directive (EU) 2016/680 is too broad for the classification of AI as high risk, and whether as an alternative, a definition should be included in the Regulation itself or a concrete description of circumstances that are considered critical should be included in Annex III. In this context it is important to Germany, for example, for this definition not to include in particular the tasks of an FIU, in the sense that “The core function of an FIU is the receipt, analysis and transmitting of suspicious transaction reports identified and filed by the private sector”. This also applies in particular if these suspicious transaction reports are considered in association with financial transactions by natural persons. How do the Commission and the other Member States judge the need for clarification of point 6, letter (f)?

d) Derogation from regular conformity assessment procedures in urgent cases to protect high-level legal interests in the field of law enforcement

The proposal from the Commission guarantees compliance with the requirements for high-risk AI systems by imposing the obligation to carry out a conformity assessment, among other things.

In its proposal for a Regulation, the Commission has recognised that particular situations can justify derogation from the regular conformity assessment procedure. Article 47 (1) of the proposal permits provisional authorisations if the delay caused by carrying out the conformity assessment procedure poses a risk to other high-level interests.

In addition, with Article 47 (1a) of the proposal, the presidency has suggested a further derogation provision specifically for law enforcement authorities that, in particularly urgent situations, allows for the provisional putting into service of high-risk AI systems without prior authorisation by the market surveillance authority.

Germany is of the view that the presidency's supplementary proposal is generally reasonable. However, Germany considers that the requirements of the derogation regulation in Article 47 (1a) of the proposal are too unspecific. In particular, it remains unclear exactly what "duly justified situation of urgency for exceptional reasons of public security" means. Discussions are under way in Germany regarding whether, from the point of view of protection of fundamental rights, provisions should be included for safeguards and an arrangement for the legal consequences of violations of the rule. Moreover, discussions are also under way in Germany on whether the market surveillance authorities should be informed before the provisional putting into service in such cases, to enable verification of the criteria. From an operational point of view, the proposal also does not yet answer the question of the usability of intelligence obtained from the deployment of a non-certified AI system in urgent cases. Germany sees a need for this question to be addressed in the proposed regulation.

As a whole, regulation of AI should include provisions to balance fundamental rights aspects with operational aspects in these urgent cases, providing legally secure certification that ensures that data and information from these systems can be used; in doing so, the AI Act should in particular stipulate the conditions under which the certification procedure affects the legitimacy of measures based on the provisional deployment of AI systems.

e) Confirmation by a minimum of two persons (Article 14 (5) of the AI Regulation)

The German security authorities are concerned about whether the two-person rule in Article 14 (5) of the proposal could encompass application scenarios in the field of law

enforcement that are already in place and that represent procedures in accordance with Annex III no. 1 (a) of the proposal; this could in particular also affect situations in which the authorities with powers of enforcement currently deploy one person. As a result, the two-person rule in the AI Regulation could lead to disproportionately high implementation costs. It also leads to the fear, for example, that identification searches using fingerprints in the SIS or VIS during border controls (for example if a border is crossed without documentation) could be included in the scope of the regulation.

If the rule also includes standard measures as defined above, then discussions are under way in Germany regarding the weighting of the two-person rule in relation to potential measures and decisions that law enforcement officers can take individually in ad hoc situations. Officers can, in principle, implement very extensive measures, right up to the application of direct force, on the basis of individual decisions without the involvement of an additional officer. What are the views of the Commission and the other Member States on the issues mentioned above? Germany requests an explanation of the legal basis of Article 14 (5).

f) Norms and standards in the conformity assessment procedure (Article 40 and 41 of the proposal)

There are specific requirements for IT security, trustworthiness, and the protection of data and fundamental rights in the field of security, in addition to specific sectoral requirements. Discussions are under way in Germany regarding whether it is possible to ensure that these specific requirements in the field of security be taken into account within the standards under Article 40 and the specifications under Article 41 of the proposal. What are the views of the Commission and the other Member States on this?

g) Transitional arrangements for the EU information systems listed in Annex IX

Germany also suggests excluding large-scale IT systems established by the legal acts listed in Annex IX from the obligations of users of high-risk AI systems set forth in Article 29 (in connection with Article 12 and Article 11) regardless of the date the systems were placed on the market or put into service, since these systems are already regulated with regard to those obligations, and the obligations laid down in the AI Act may conflict with the obligation laid down in existing legislation.

If the amendment of these legal acts leads to a significant change in the design or intended purpose of the AI system, it then should be considered as a question of legal technique if any obligations of users of high-risk AI systems under the AI Act should be implemented directly within the legal acts listed in Annex IX itself.

Furthermore, the suggested exemption is without prejudice to Article 83 (2) of the Commission's proposal, according to which the requirements laid down in this Regulation shall be taken into account in the evaluation of each large-scale IT system established by the legal acts listed in Annex IX, to be undertaken as provided for in those respective acts.

h) Training data

Germany shares the aim of developing AI systems that are as free of errors and unbiased as possible. This applies in particular in the field of law enforcement, which is of specific relevance to fundamental rights. Discussions are under way in Germany of the extent to which the rules on training data quality should be revised in order to achieve these aims. In this regard, the field of law enforcement, as well as being of specific relevance in regard to fundamental rights, is also particularly affected by the special requirements for training data in regard to data protection and confidentiality interests. Discussions are under way in Germany regarding how to ensure that the provisions in the proposed regulation are in line with the most up-to-date technology in the development of AI and the latest scientific standards, to ensure AI that is as free of errors and as unbiased as possible. This brings up the question, for example, of the extent to which a provision on training data that is "free of errors" reflects the latest scientific research on developing AI that is as free of errors and as unbiased as possible. What is the view of the Commission and the other Member States on this matter?

2. Specific matters in the field of migration

a) Adaptation and differentiation in classification as high-risk AI (Annex III)

The categorisation proposed by the Commission of AI systems deployed by migration authorities as high risk in accordance with Annex III point 7 of the proposal was already discussed in detail during the Council negotiations. The presidency has already proposed amendments in this regard which are still under discussion among the Member States. The following point is currently under discussion in Germany:

- Letter (d): We request further clarification. The description of AI systems covered by letter (d) should be clear-cut. It must be ensured that systems without risk to health, safety or fundamental rights are not covered. For Germany, it is very important that letter (d) is defined more narrowly in this respect. At the same time, systems that pose a risk to the abovementioned protected interests must remain covered.

b) Non-publication of high-risk AI applications (Article 60 and 61 of the proposal)

In regard to the migration authorities, too, the German Federal Government is concerned that public access to the EU database of high-risk AI applications provided for in Article 60 (5) of the proposal could clash with justified security interests of the Member States. In the field of migration, this could particularly affect AI systems that are used for the analysis of possible travel movements. Do the Commission or the other Member States share this assessment? Should an exception be included in this regard in Articles 60 and 61 enabling the Member State in question under certain conditions, which must first be defined in more detail, to refrain in individual cases from publishing AI applications where security interests are at odds with this?

c) Transitional arrangements for the EU information systems listed in Annex IX

Please refer to point 1 (g) of this paper.

d) Training data

Please refer to point 1 (h) of this paper.