

# Position Paper

---

on the proposal for an EU Artificial Intelligence Act  
COM(2021) 206 final



## 1. Background

---

For more than 100 years, the German Retail Federation (Handelsverband Deutschland - HDE) has been the umbrella organisation of the German retail sector - the third largest economic sector in Germany - with a total of three million employees and an annual turnover of more than 535 billion euros. It represents the concerns and interests of around 300,000 retail companies - of all sectors, locations and company sizes. With 50 million customer contacts daily, the retail sector supplies its customers with the complete range of products - via all sales channels.

In April 2021, the European Commission presented a comprehensive proposal for the regulation of artificial intelligence (AI), which is unique in terms of the depth and breadth of regulation. With the draft, the Commission follows up on its "White Paper on Artificial Intelligence" and wants to guarantee that AI is safe, lawful and in line with fundamental rights in the EU. While AI is a rapidly evolving and strategically important technology that offers enormous opportunities, some applications pose significant risks. The overall objective, according to the Commission, is to promote the use of trustworthy AI in the EU.

Against this background, the regulation aims to give the use of AI a uniform EU-wide framework in line with fundamental rights and to establish the EU as a technology leader. With the draft regulation, the Commission thus proposes to ban certain AI applications and to allow selected, high-risk AI technologies in the internal market only after they have been reviewed - i.e. only high-risk AI systems that have undergone quality management and conformity assessment procedures are to be allowed in the EU. Most other AI applications will have to comply with transparency and labelling requirements.

## 2. HDE Position

---

The commercial use of AI is clearly emerging and will advance rapidly. A promising field of application for AI technologies is the retail sector – for both online and brick-and-mortar retail. Because of their interface function, retailers find themselves in a complex network of relationships between customers, manufacturers, logistics providers and platforms. In order to survive in today's competitive environment, it is important to understand optimally customer needs and to fulfil them as efficiently and precisely as possible. AI systems can process highly complex tasks involving large amounts of data in real time and generate an optimal solution that meets the requirements. In a fast-moving and dynamic (retail) world, they can learn from and with the customer and adapt services to the customer's wishes in a resource-saving manner, quickly and effortlessly for the end user.

Customers in the digitised world demand tailor-made offers, confidently put the focus on themselves and want to experience their individual retail worlds. Thus, 65% of Germans are loyal above all to providers who tailor their offers specifically to the needs and preferences of the customer. To meet this demand, 45% of retailers plan to use artificial intelligence in the next three years. Accordingly, AI is a success factor for digitalisation and for future business models in retail.



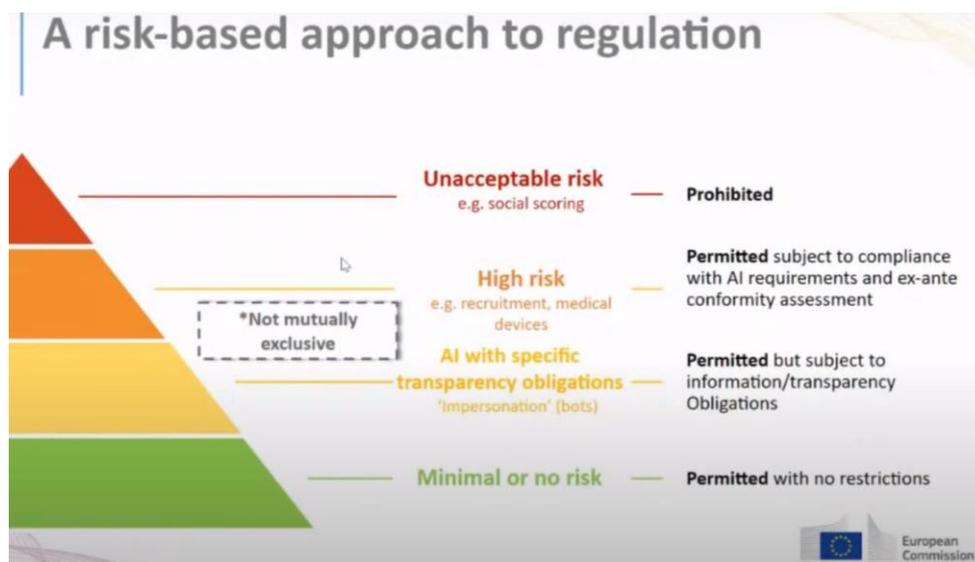
The [application areas of AI in retail are diverse](#): intelligent systems can accompany the entire business process from head office to logistics to the shop floor and according customer experience. For example, HDE's AI Deep Dives show how [smart shelves for inventory monitoring](#), [intelligent counters](#) or a [product magnifier with augmented reality \(AR\)](#) already make buying and selling easier for customers and retailers. Certainly, these technologies are not relevant for all retailers. However, standard examples such as [inventory management with the help of intelligent systems](#) (regardless of whether retailers choose online or brick-and-mortar sales channels), smart route planning in logistics, the digital changing room at the point of sale and [visual product search](#) in customer contact can be widely used.

As HDE, we are convinced that intelligent applications are an opportunity for future-oriented retailing. Furthermore, we expressly support the Commission's goal of promoting the use of trustworthy AI in the EU economy. This is the key to the success of this technology on our continent.

#### a) General, risk-based regulatory approach

We welcome that the Commission proposes a risk-based and technology-neutral regulatory framework, assessing applications according to their intended use and focusing on achieving desirable outcomes rather than regulating individual tools.

In contrast to the proposal of the German Data Ethics Commission of 2019, which envisaged a multi-level regulatory model with graduated requirements depending on the "potential for harm", the Commission regulates only a few categories of AI: applications that are so risky that they are banned, high-risk and low-risk AI. We support this risk-based approach, which at the same time is not too complicated and multi-layered. A large part of AI applications in Europe would remain largely unregulated and manufacturers could bring many further applications to market by self-assessment.



However, as with any kind of risk-based regulation, it is essential that "high-risk AI applications" are defined and delimited in a clear, future-proof and legally secure manner. We see good approaches



with the lists of laws and uses in Annexes II and III of the regulation. However, it is also important to ensure that the boundaries between the categories are clearly defined and remain easy for small companies to delineate independently: When does a chatbot that is actually of minimal risk (which in principle is only subject to the transparency requirements under Article 52) qualify as a prohibited AI if it potentially causes "physical or psychological harm"?

It is also important to us that unnecessary duplication is avoided. It must be noted that the General Data Protection Regulation (GDPR) only came into force in 2018 and it will take time for its full effect to unfold. Therefore, matters already regulated by the GDPR should be taken into account and not regulated twice. Many of the proposed requirements are already regulated in the GDPR and are applied in practice, such as the record-keeping requirements (see below).

### I. Prohibited use of AI (Art. 5)

The proposal contains a list of AI applications that should be banned in the EU because they "contradict Union values ... and Union fundamental rights" (recital 15). The list includes, among others, AI systems that manipulate negatively human behaviour, opinions or decisions, or inflict physical or psychological harm, target vulnerabilities in vulnerable groups, engage in social scoring or can be used for real-time remote biometric identification in law enforcement (with exceptions).

As an example of a product that will be banned in the future, the Commission mentions, for example, "toys with a voice assistant that encourage minors to engage in dangerous behaviour". However, it is completely open what is to be regarded as "dangerous behaviour" and it is doubtful that this is always accompanied by "physical or psychological harm". This definition in particular must therefore be improved, because it cannot be ruled out that recommendation systems used in retail, which are necessary for the customer to navigate through large masses of information, could also fall under this (if they are based on AI). Accordingly, it must be ensured that the use of "subliminal techniques beyond a person's consciousness ... to materially distort a person's behaviour in a manner that causes or is likely to cause ... physical or psychological" (Art. 5(1a)) does not include AI-based algorithms for [automatic product recommendations](#).

Personalised product recommendations, special offers and discounts take into account individual wishes and needs of customers and can thus play out relevant offers. This is an added value for consumers that we should appreciate and protect in order to deal with the confusion and amount of information on the internet. Intelligent product display and website design presents relevant content to the customer in a clear way, for example by filtering product reviews by topic.

### II. High risk AI applications (Art. 6, Annex II & III)

In addition, the proposal names two groups of AI systems that are to be classified as high-risk. However, these high-risk AI applications are not to be completely banned, but their use is to be subject to certain requirements and an authorisation procedure:



1. AI systems that are used in products or are themselves products that fall under the EU law listed in annex II. The EU regulations on machinery, toy safety, radio equipment and - with some exceptions - personal protective equipment and medical devices are of particular relevance to retail.

2. AI applications mentioned in the list in Annex III. The following are likely to be relevant for retail:

- AI systems to be used in education and vocational training
- AI systems that are to be used for the recruitment, evaluation and promotion of personnel.
- AI systems that are to be used for assessing the creditworthiness of individuals
- AI systems to be used for remote biometric identification of people in public spaces.

In the areas of education and training, as well as employment and human resource management, a legally secure framework can make sense in principle, for example to promote the willingness of commercial enterprises to develop and use innovative and employee-friendly AI applications, which represent important tools for increasing productivity and effective division of labour between humans and machines. However, the blanket assumption that AI applications in these fields are associated with a high level of risk leads to considerable legal uncertainties for companies and also means disproportionate overregulation. An overly broad definition of high-risk AI applications would have a negative impact on the level of innovation and application and would be counterproductive to the highest degree. It would therefore be highly recommended that the areas listed in Annex III be limited to specific use cases with actual high risk.

With regard to the last point, it must also be ensured that only *passive, mass identification from a distance* is covered and not the active identification of individual persons, e.g. at the point of sale. Only in this way can certain biometric authentication systems remain possible, which contribute to significant innovations in retail, such as payment by fingerprint or cashierless shops. These should continue to be possible in the sense of promoting innovation and facilitating processes for customers and suppliers.

Furthermore, the distinction between "biometric remote identification" on the one hand and "biometric categorisation system" (Art. 52 para. 2) on the other hand must be clear and unambiguous. In the latter case, no collected data is compared with stored data - i.e. identified - but only a rough categorisation is carried out, e.g. on the basis of age. We therefore consider the fact that only transparency requirements according to Article 52 should apply to "biometric categorisation systems" to be appropriate. Thus, the addition of "and categorisation" in Annex III under point 1 should be deleted, especially since no concrete case of application is listed and it is only a placeholder that could easily be (re-)included in a later revision of the regulation.

### III. Further AI applications (Art. 52)

Other AI applications that are not banned or classified as high-risk AI must comply with certain transparency or labelling requirements - if they interact with humans. Chat bots and deep fakes, for example, fall into these categories.



In principle, this should be supported, as such systems are common customer communication practice and contribute to a speedy and smooth problem resolution, which is in the interest of both customers and retailers. The way in which machine communication is labelled must be clear, simple and uniform in order to avoid confusion on the part of consumers and businesses and not overburden small and medium-sized enterprises. SMEs in particular can benefit from the use of AI-based chatbots, as they usually have neither human nor financial resources for human communication with a wide reach. Here, the regulation must not disadvantage the weakest market participants.

### b) Scope / definition of AI

The scope of the regulation is broad. An "AI system" is defined as software that has been developed by means of certain techniques and approaches such as machine learning and autonomously generates results that influence the living world according to humanly specified goals (Art. 3 in conjunction with Annex I).

Accordingly, this AI definition encompasses almost every algorithm, i.e. it is extremely comprehensive, so that a very large number of software applications would fall under the legal framework. Whether it is a search engine or internal trend detection for market analysis, whether it is automated energy management or a cashierless supermarket - all these examples undeniably have different influences on people's lives. Nevertheless, they fall under the scope of the regulation. Depending on how the risk-based approach is ultimately designed, the broad definition of the term AI could be sufficient. However, AI applications are developing rapidly. It cannot be ruled out that the definition will be flooded and thus empty of content within a decade.

We therefore advocate that the definition be clarified and narrowed to focus on the areas where the highest and most far-reaching risks are expected. As it is currently worded, the definition would encompass most modern software applications and make it extremely difficult to assess which areas fall within the scope of this regulation. There also needs to be a clear distinction between regulating AI and regulating algorithms. The draft law does not make this distinction. It must be made clear that you cannot regulate algorithms, which are nothing more than mathematical formulas.

### c) Extra-territorial scope

To ensure a level playing field, the new legislation must also apply to providers based in countries outside the EU if they offer AI systems in the internal market, as is already the case with the GDPR, for example. HDE therefore expressly welcomes the fact that the regulation also covers providers based outside the EU who place or operate AI systems on the EU market or use AI results here (Art. 2(1)). However, it is important to ensure that these requirements not only exist on paper, but are also effectively implemented in practice.

Whenever we develop regulations on AI, we need to bear in mind that they will apply at an early stage for many SMEs, start-ups and other companies in the EU. The regulations will put relatively more burden on these players than on larger companies that have the expertise and resources to cope with the additional requirements. Moreover, companies outside the EU may already be growing strongly in



their home markets and will only have to comply with these rules once they expand into the EU single market, whereas EU companies will have to apply the rules immediately.

We must therefore measure the obligations imposed against their cost and benefit and design the legal framework in a way that European companies nevertheless have the opportunity to become international pioneers in the field of AI. This is also underlined by a new survey: The Center for Data Innovation has calculated that the proposed draft could cost the European economy €31 billion over the next five years and reduce AI investment by almost 20%. A small or medium-sized company using a high-risk AI system could incur compliance costs of up to €400,000, resulting in a 40% drop in profits<sup>1</sup>.

#### d) Requirements for high-risk AI (Art. 8 ff.)

The high-risk AI applications defined in Article 6 must meet certain requirements, taking into account their intended use. These include the establishment of a risk management system (Art. 9), the use of high quality data sets (Art. 10), documentation and records for review (Art. 11 & 12), transparency and provision of information to users (Art. 13), human supervision (Art. 14), and robustness, accuracy and safety (Art. 15).

##### I. Recording obligations (Art. 12)

Recording obligations are important and give developers the possibility to retrace their steps. They also allow to establish a relationship of trust with end-users. Recording obligations should, however, contain information that also represents added value for users and that can be recorded in an uncomplicated manner. In our view, the following information - among others - could be made available in the sense of recording obligations and with a benefit for end users and developers:

- Artificial Intelligence Architecture
- Resources used
- Problem statement and solution approach
- Computer-implementable instructions
- Responsible use of AI & associated data/processes e.g. re:
  - Carbon footprint of resources vs. benefits.
  - No discrimination in AI use to harm or oppress one group
  - No AI exploitation of humans and animals
  - No detection of diseases through user behaviour
- Data compliance with DSGVO
- Transparent documentation of data
- Verification and minimisation of bias (language, gender, etc.) to the best of our ability

Finally, we believe that the duration of the record-keeping obligation should be aligned with the GDPR. The GDPR is the blueprint for all further digital and data-related legislative proposals. Therefore, the

---

<sup>1</sup> <https://www2.datainnovation.org/2021-aia-costs.pdf>



duration of the data retention obligation should also be adapted and not go beyond existing obligations. Storing data that no longer has any use can lead to confusion and additional effort without adding any value.

## II. Protection of trade secrets

Especially in the context of documentation and transparency and regarding reference to algorithms in Recital 46, we would like to point out that the protection of business secrets must be maintained at all times in this context.

Whether online or offline, algorithms help shape modern retail companies. They enable [the product range to be adapted to the individual needs](#) and wishes of the customer, allow the risk of non-payment to be estimated and [optimise sales forecasts](#) and delivery routes. Algorithms have thus become an important differentiating feature, especially in retail.

Regulatory inconsistencies can mutate into competitive disadvantages for European retailers if different legal standards are applied to offline, online and smart, i.e. AI operated. On the one hand, the existing legal framework already offers consumers adequate protection. On the other hand, we cannot demand the disclosure of trade secrets in the digital world that would be protected in the offline world.

This is because there is a risk of competition being restricted if the core content of algorithms has to be disclosed. Those who have to disclose these lose the incentive for further developments and thus the connection to global competition. Moreover, the efficiency of such a review can be questioned, since algorithms are often complex, change frequently and contain random moves. We therefore favour a principle-based approach that sets out ethical principles for fair algorithm use, as developed by the Commission's independent expert group on artificial intelligence in the ethical guidelines for AI.

## III. Harmonised standards

Another potential problem arises from the fact that the proposal refers to harmonised standards that do not yet exist. Corresponding standards must be worked out and specified quickly. It would be desirable to submit standardisation applications for the AI Act already before the official publication of the Act. The participation of all interested stakeholders in the development of these standards must be ensured. Existing standards should be used and further developed.

### e) Changes to the regulation

On the basis of Article 4 in conjunction with Article 73, the Commission can amend definitions - including the central AI definition - by delegated act. The list of high-risk AI applications from Annex III is also to be amended by delegated act (Article 7). However, this should both be done in an orderly parliamentary procedure.

In an earlier version of the proposal, the Commission was supposed to consult both the European Artificial Intelligence Board and a public stakeholder consultation for such a change. These requirements have regrettably been deleted and should definitely be reintroduced - especially when it comes to additions of high-risk AI applications in Annexes II and III.



Even better than a consultation would be - analogous to e.g. the Regulation on Explosive Precursors 2019/1148/EU - to provide the Commission with a Standing Committee, in which, in addition to representatives of the Member States, stakeholders can also be regularly consulted on the question of the extension of the high-risk list. Originally, such an expert group (to advise the Board) had also been envisaged, but was deleted from the proposal.

#### f) Conformity & approval

In order to be able to offer high-risk AI applications, the provider carries out a conformity assessment to demonstrate compliance with the requirements (Art. 43). Also, a declaration of conformity must be drawn up for the corresponding products (Art. 48) and a CE marking must be affixed (Art. 49).

We welcome the alignment with the New Legislative Framework (NLF) and the EU product safety. It must be possible to integrate the new requirements into existing processes with as little additional effort as possible and the greatest possible consistency with existing regulations should be guaranteed. This applies in particular to the coordination and cooperation of the authorities involved (market surveillance, nationally competent AI authority, conformity assessment bodies, standardisation bodies, etc.) in the interaction between the AI Act and the existing legislation of the NLF. But also with regard to the distinction between "operator" and "user", coherence should be ensured against the background of the upcoming debate on product liability. One should ensure that the AI proposal and the revision of the Product Liability Directive are consistent on these terms.

#### g) Further points

- Support for SMEs: The goal of AI is to develop a system that can make autonomous decisions without human influence and supervision. Security is essential, but the essence of the technology should be considered. The freedom for autonomous decision-making should be given to a certain extent. We therefore expressly welcome the fact that AI systems can be tested in regulatory "sandboxes" before they are launched (Art. 53), in which companies and developers can test products in a safe way before they are brought to market, and that SMEs and start-ups in particular should be given special support (Art. 55).
- Fines (Art. 71): The maximum level of fines that Member States can impose for infringements of the Regulation is set at 10/20/30 million euros for each of three categories of infringements, or two/four/six percent of the annual worldwide turnover. The €30 million/6% fines apply, for example, to developing, offering, introducing and using prohibited AI applications. We consider fines at this level to be disproportionate and advocate bringing them in line with the level of the GDPR and thus reducing them to a maximum of four percent of annual turnover.
- Guidelines for developers: Since the regulations are primarily written for lawyers, we would welcome it if the Commission could present an application-oriented guideline after the conclusion of the legislative process, in which the regulations are "translated" in a practical and easy-to-understand manner for AI developers, e.g. with corresponding checklists and step-by-step instructions. The guidelines could help developers answer questions such as when an AI application poses a high risk or how to ensure that data sets do not contain bias.



### 3. Conclusion

---

Artificial Intelligence is a fundamental innovation that will change numerous business models and enable new ones. What applies in the analogue economy with human decisions should also be considered in the digital economy with data-based decisions. Existing regulations should therefore be reviewed and only adapted to the development triggered by AI systems if there is a proven need. It must be ensured that SMEs in particular can also make practical use of externally generated "AI as a service", as they will often not be in a position to develop AI systems themselves.

HDE therefore welcomes the Commission's risk-based and balanced proposal, which explicitly takes into account the interests of the economic actors concerned - especially SMEs - and balances their potential burden from possible regulation against the benefits. The explicit focus on legislative coherence is also positive. This approach must be consistently pursued in the further course of the legislative process.

After all, when it comes to AI, we are moving in an area of competitive tension and must offer Europe as an innovation space for technological developments and economic growth instead of making progress more difficult without good reason.

The following substantive points are of central importance to us:

- It is paramount that "high-risk AI applications" are defined and delimited in a clear, future-proof and legally secure manner. We see good approaches with the lists of laws and purposes in Annexes II and III. However, it is also important to ensure that the boundaries between the categories are clearly defined and that they can be easily demarcated independently, even for small companies.
- It must be ensured that Article 5(1a) does not prohibit AI-based algorithms for automatic product recommendations, because these take into account the individual needs of customers and can thus provide relevant offers. This is an added value for consumers that we should value and protect in the confusion of information.
- With regard to remote biometric identification, it must be ensured that only passive, mass identification from a distance is covered and not the active authentication of individuals. Only in this way can certain systems remain possible that contribute to significant innovations in retail, such as payment by fingerprint. These should continue to be possible in the sense of promoting innovation and facilitating processes.
- Furthermore, the distinction between "biometric remote identification" and "biometric categorisation system" must be clear and unambiguous. In the latter, no collected data is matched with stored data, but only a rough categorisation is made, e.g. based on age. We therefore consider the fact that "biometric categorisation system" should only be subject to transparency requirements under Article 52 to be appropriate.
- In the areas of education and training, as well as employment and human resource management, a legally secure framework may be appropriate in principle. However, the blanket assumption in the regulation that AI applications in these fields of application are associated with a high risk



unnecessarily leads to considerable legal uncertainties for companies and also means disproportionate overregulation. An overly broad definition of high-risk AI applications in Annex III would therefore have a negative impact on the level of innovation and application and would be counterproductive. It would therefore be recommended to limit the areas listed in Annex III to specific use cases with actually high risk.

- It is to be supported that systems such as chatbots, which are common customer communication practice and contribute to a smooth problem solving in the interest of customers as well as traders, only have to fulfil labelling requirements. The type of labelling must be clear, simple and consistent in order to avoid confusion on the part of consumers and businesses and not overburden SMEs.
- SMEs in particular can benefit from the use of AI-based chatbots, as they usually have neither human nor financial resources for human wide-ranging communication. Here, the regulation must not disadvantage the weakest market participants.
- To ensure a level playing field, the new legislation must also apply to providers based in countries outside the EU if they offer AI systems on the single market. In addition, it is important to ensure that these requirements do not only exist on paper, but are effectively implemented in practice.
- In connection with the documentation and transparency requirements for high-risk AI applications, we would like to point out that there is a risk of distortion of competition if the core content of algorithms has to be disclosed. Those who have to disclose these lose the incentive for new developments and thus the connection to the global competition.
- Recording obligations are important and give developers the opportunity to retrace their steps; they also make it possible to establish a relationship of trust with end users. Recording obligations should, however, contain information that also represents added value for users and that can be recorded in an uncomplicated manner.
- Changes to the regulation - especially with regard to the classification as high-risk AI - should not be implemented by delegated act, but rather in the parliamentary procedure. In the case of such changes, at least a public stakeholder consultation should be carried out, or better still a Standing Committee of Experts should be created, in which stakeholders can also be consulted on the question of extending the high-risk list.
- We welcome the alignment with EU product safety legislation. It must be possible to integrate the new requirements into the existing processes without additional effort, and the greatest possible consistency with the existing regulations should be guaranteed. This applies in particular to the coordination and cooperation of the authorities involved.
- We consider the fines to be disproportionate and plead for them to be adjusted to the level of the General Data Protection Regulation and to be reduced to a maximum of 4 percent of the annual turnover.
- We would like to call on the Commission to present a practical and comprehensible guideline for developers after the conclusion of the legislative process.