Open letter to the US company Open AI as developer of the text robot ChatGPT

By Stefan Brink, Rolf Schwartmann and Axel Voss

Dear Sir or Madam,

the use of ChatGPT and similar products using Artificial Intelligence (AI) from your company is causing concern and is increasingly coming under criticism in Europe as well as beyond.

Not only data protection authorities, but also voices from business, government and academia recognize that the uninformed use of such software is becoming a problem. This highly topical technology collides with many legal rights and legitimate interests that have a firm place in our European system of values: What about the transparency of your algorithms? How reliable are the results of your software, which seem so plausible? What protection do you provide against results that are not age-appropriate? How do you protect our societies from distortions caused by the formation of bubbles, the amplification of centrifugal forces, and even the widespread loss of jobs? How do you protect our personal rights, the intellectual property of others, and how do you prevent fake news?

The European Union is a community of values, characterized in particular by the fact that technologies are not used because they exist or because individuals expect advantages from them, but because there is a democratically legitimized, value-oriented decision in favour of the technologies - which may only be used to a limited extent. This has proven successful, for example with the EU's General Data Protection Regulation, and Europe should stick to it.

Legislators in the European Union also see a need for short-term regulatory action. At the same time, companies and public bodies that want to use your brand-new software are themselves responsible for this use in terms of data protection law and are dependent on factual knowledge for responsible handling of your products.

The fact that the data protection authority in Italy has summarily blocked the ChatGPT service for use there is a far-reaching step. In Italy, it is currently no longer possible to access the service at all. Whether it was necessary to cut off all people there from the new technology is debatable. In our view, this step is inappropriate at the moment because it is premature. The supervisory authorities do not yet have a clear picture of your products and how they work. Government supervision should not act "out of the blue".

In our view, the service should not be banned across the board in Europe but should be integrated into the existing legal framework. Currently, neither the functionality of the technology is open, nor the purposes for which the software uses entered data, nor which data was fed in at all and how the bot is programmed. A deep neural network that throws out probability calculations in human language that simulate knowledge indistinguishable from human knowledge needs to be explained in detail by its provider. So far, you have owed us that.

For the service to be used responsibly, we need to know the pool of training data from which the results are generated. We must be informed about the origin of the training data as well as about the parameters that were decisive in programming the bot. This is the only way to assess the risk of discrimination and manipulation of the product results and misuse of the database. We need this knowledge to ensure that humans can review, evaluate and, if necessary, reject the bot's results - basics for the controllability of your offering. We also need the knowledge to be able to create the technical conditions for controlling their products.

In order to check the permissibility under data protection law, we also need to know their exact processing purposes and how the service is to be financed. For what purposes is data processed and stored by which parties, and how is it secured. To what extent is the data entered, which allows deep insights into the psyche of users similar to search engine queries, anonymized or pseudonymized?

As far as can be seen, there is also no convincing solution so far for your responsibility and liability for incorrect or even illegal results.

Since the use of your software is just as effective in private life as it is in business, schools and universities, there is an acute need for action simply because of this enormous broad impact of your products. Explain your products to us!

To ensure that your offer does not have to be banned and to avoid fines for you and users, we are impatiently awaiting your reply as soon as possible at info@gdd.de.

Yours sincerely

Dr. Stefan Brink, Berlin

Professor Dr. Rolf Schwartmann, Cologne

MEP Axel Voss, Brussels

Dr. Stefan Brink *is Executive Director of the Scientific Institute for the Digitization of the Working World (Berlin) and was previously State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg.*

Professor Dr. Rolf Schwartmann *is Head of the Cologne Research Center for Media Law at the TH Köln and Chairman of the Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. (Society for Data Protection and Data Security).*

Axel Voss *is a Member of the European Parliament and EPP Rapporteur for the Artificial Intelligence Regulation and European Parliament Rapporteur for the Artificial Intelligence Liability Directive.*