COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2023

Patrick Wellens (patrickwellens@hotmail.com) is currently working as a Compliance Manager for a division of a multinational pharma company, based in Zurich, Switzerland. He is the Vice-Chair of Ethics and Compliance Switzerland and co-chair of the working group "life sciences."

European Union perspective on artificial intelligence/ChatGPT and how it relates to compliance

By Patrick Wellens, CCEP-I, CIA, CFE, CRMA, MBA

ChatGPT, Bard, and other artificial intelligence (AI) technologies will affect many industries and revolutionize the way we work. To name a few:

- AI can generate automated customer service responses by answering FAQs.
- AI can generate unique content for marketing campaigns like social media or email.
- AI can aid students with learning by using digital tools for research.
- AI can help legal professionals draft legal documents, contracts, and communications to clients, opposing counsel, and courts.
- AI can help human resources departments by improving the onboarding experience for new hires, scheduling training sessions, answering common questions on insurance/payroll/benefits, or identifying potential candidates who would be a great fit based on (industry) experience or skill set.

Does this mean that ChatGPT can be used without limitations? To answer this question, it is important to understand the regulatory framework around the use of AI.

What is the regulatory framework for the use of AI?

The use of AI is defined in several laws, directives, and guidelines. Here are some of the most significant.

Artificial Intelligence Act

The Artificial Intelligence Act is based on several principles.[1] The use of AI technology must be in line with European Union (EU) values and fundamental rights.[2] The charter of fundamental rights of the EU defines the universal values of human dignity, freedom, equality, and solidarity; it is based on the principles of democracy and the rule of law. This contains principles on nondiscrimination and gender equality.

AI technology must comply with existing General Data Protection Regulation (GDPR),[3] EU Data Governance Act,[4] EU strategy for data,[5] and AI Liability Directive.[6]

The Artificial Intelligence Act applies a risk-based approach by defining AI services that create unacceptable,

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

high, and low or minimal risks. AI services that materially distort a person's behavior in a manner that causes (or is likely to cause) that person or another person physical and/or psychological harm; that exploits vulnerabilities of a specific group of persons due to their age, physical disability, or mental disability; or that evaluate or classify the trustworthiness of natural persons over time based on social behavior or known/predicted personality characteristics with the social score leading to detrimental or unfavorable treatment of certain natural persons/groups are forbidden.

AI systems also have a transparency obligation. AI systems shall be designed and developed in such a way that their operation is sufficiently transparent to enable users to interpret the systems' output.

AI systems should have human oversight. High-risk AI systems should be designed and developed in such a way that natural persons can effectively oversee them during the period in which the AI system is in use, intending to prevent or minimize the risks to health, safety, or fundamental rights. The Artificial Intelligence Act defines the following requirements for high-risk AI systems:

- A risk management system shall be established.
- Governance over data to ensure data sets are relevant, representative, free of errors, and complete in view of intended purpose of an AI system.
- Technical documentation exists.
- AI systems shall be designed/developed to ensure their operation is sufficiently transparent to interpret system output.
- AI systems shall be designed/developed so that they can be overseen by natural persons when in use.

EU guidelines on ethics in AI

The EU guidelines on ethics in AI, created in 2019, later resulted in the foundation for the Artificial Intelligence Act.[7]

GDPR

The GDPR was created in 2016 and went into effect in May 2018. The GDPR regulates the principles to be followed when processing personal data. For example, under GDPR (Article 22), a data subject has the right to object to automated processing of their data by a chatbot.

(Revised) Product Liability Directive

The Product Liability Directive (PLD), introduced in 1985, is a common set of rules enabling harmonization and an equal level of protection of consumers throughout the EU using the concept of no-fault-based liability (this means strict liability where producers are responsible for defective products regardless of whether the defect was their fault) for damage caused by defective products.

To be compensated under PLD, the burden of proof for the injured person consists of showing the product was defective, damage was suffered, and a causal relationship exists between the damage and the defective product.

The revised PLD sets a wider definition of product and clarifies that software (including software updates) must be considered a product in the scope of the directive. The revised PLD would apply if the defective product causes physical harm, property damage, or data loss. If manufacturers and software developers do not mitigate

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

cybersecurity risks, then this lack of safety requirement must be considered by a court in evaluating whether a product is defective. The revised PLD also alleviates the burden of proof for victims under certain circumstances.

AI Liability Directive

One of the most crucial functions of civil liability rules is to ensure that victims of damage can claim compensation. By guaranteeing effective compensation, these rules contribute to protect the right to an effective remedy and a fair trial (Article 47 of the EU Charter of Fundamental Rights) while also giving potentially liable persons an incentive to prevent damage and avoid liability. With the AI Liability Directive, the commission aims to ensure that victims of damage caused by AI have an equivalent level of protection under civil liability rules as victims of damage caused without the involvement of AI.[8]

EU directive on unfair commercial practices

Directive 2005/29/EC regulates unfair commercial practices in business-to-consumer transactions. It applies to all commercial practices that occur before, during, and after a business-to-consumer transaction has taken place.[9]

What are the (compliance) risks when working with ChatGPT?

The following risks can be mentioned when working with generative AI.

Quality and output issues

Unfair or biased information on the web might not be properly contained within the chatbot’s algorithm. ChatGPT can produce inaccurate results.

For example, people should be wary of using ChatGPT to give them legal advice. According to an article in *Allens Linklaters*, “ChatGPT can only generate text based on patterns it has learned from the data on which it was trained. Therefore, if its training dataset does not contain sufficient resources on the particular area of law on which it is queried, the chatbot may produce a lucid and comprehendible answer, but one based on an incomplete or dated picture of the law.”[10]

ChatGPT can also fabricate convincing medical data, which makes it easier than ever to publish fraudulent research.[11]

Privacy risks

In March 2023, Italy’s national privacy regulator ordered an effective ban on ChatGPT, accusing OpenAI of “unlawful collection of personal data.” The ban was lifted in late April.[12]

Where personal data is shared with ChatGPT, one should be aware that this could lead to personal data being transferred to third parties; therefore, companies may be obligated to provide notices to customers, obtain their consent, provide them with opt-out rights, etc.

There is also the question of how companies that use ChatGPT to process personal data will deal with requests from users who want their personal data deleted.

Confidentiality risk

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website’s Terms of Use.

Companies should keep in mind that the usage rights for ChatGPT are set out in multiple documents, including the terms of use, content policy, and usage policies, which state that content provided to ChatGPT may be used to develop and improve its functionality.

Therefore, when inputting a business secret or confidential information into ChatGPT, users must be aware that they disclose that data to a third party for use for an indeterminate purpose—explicitly permitted to use it in that way—which might constitute a breach of data protected by specific laws (e.g., banking laws).

Consumer protection risk

If consumers are not aware that they are interacting with ChatGPT or they receive a document from a company that ChatGPT generated without that being clearly disclosed, there is a risk of being sued for unfair or deceptive practices.

Intellectual property risk

With regards to intellectual property, the main questions are, "Who holds the right to use the generated content by ChatGPT?" and, "Is there a possible infringement of third-party intellectual property rights when ChatGPT is 'learning'?"

Considerations on a policy on the use of ChatGPT

Each company should be evaluating to what extent the use of ChatGPT presents a risk to their organization, and based on the risk profile, a company might regulate in a policy the use of ChatGPT:

- Uses that are prohibited
- Uses that are permitted under certain conditions (e.g., obtaining authorization)
- Uses that are permitted without any authorization

It is, however, best practice that any content that includes personal data; content that constitutes a business secret or is a confidential, privileged communication; and data that may not be disclosed to third parties should not be input into ChatGPT.

It is also good practice to determine for each use of ChatGPT several criteria that would determine whether the use will be low, medium, or high risk. Employees need to be trained in permitted and prohibited use of ChatGPT, and regular monitoring needs to happen.

Companies should also include in their policy and regulate in contracts how external vendors and business partners can use ChatGPT or similar tools. Such clauses should specify when ChatGPT may be used and the consequences if the use of ChatGPT infringes on third-party intellectual property rights. The policy must also determine when external disclosure is to be made when ChatGPT generates content.

Conclusion

ChatGPT has tremendous potential to increase productivity in many industries. Nevertheless, companies must be aware of data privacy, confidentiality, intellectual property, consumer protection risk, and the risk that ChatGPT can produce inaccurate results. Accordingly, companies must determine and implement a strong governance framework to mitigate such risks.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Takeaways

- Companies should embrace artificial intelligence as a new technology with tremendous potential; however, it must be accompanied by proper guardrails to allow for safe use. This means a company should have a policy, users must be trained on permitted use, and monitoring of use should happen.
- Companies must be aware of data privacy, confidentiality, intellectual property, consumer protection risk, and the risk that ChatGPT can produce inaccurate results. Therefore, companies should conduct a risk assessment and determine prohibited and permitted uses.
- Any content that includes personal data; content that constitutes a business secret or is confidential, privileged communication; and data that may not be disclosed to third parties should not be input into ChatGPT.
- Companies should regulate in contracts how external vendors and business partners can use ChatGPT or similar tools. Such contractual clauses should specify when ChatGPT may be used and the consequences if the use of ChatGPT infringes on third-party intellectual property rights.
- In the European Union, companies must be aware of the principles laid down in the Artificial Intelligence Act and Product Liability Directive.

[1] European Commission, *Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, COM(2021) 206 final, 2021/0106(COD), April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

[2] European Union, *Charter of Fundamental Rights of the European Union*, Oct. 26, 2012, 2012/C 326/02, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN.

[3] Council Regulation 2016/679, *General Data Protection Regulation: GDPR*, 2016 O.J. L119., https://gdpr-info.eu/.

[4] European Union, *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act),* June 3, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.

[5] European Union, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A European strategy for data*, COM (2020) 66 final (Feb. 19, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1582551099377&uri=CELEX:52020DC0066.

[6] Tambiama Madiega, *Artificial intelligence liability directive*, European Parliamentary Research Service, PE 739.342, February 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

[7] Tambiama Madiega, *EU guidelines on ethics in artificial intelligence: Context and implementation*, European Parliamentary Research Service, PE 640.163, September 2019 https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.

[8] European Commission, *Proposal for A Directive Of The European Parliament And Of The Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive),* COM (2022) 496 final (Sept. 28, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.

[9] European Commission, *Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules*, L 328/7, December 18, 2019, https://eur-lex.europa.eu/eli/dir/2019/2161/oj.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website’s Terms of Use.

[10] Gavin Smith et al., “ChatGPT in law: unlocking new opportunities while managing the risks,” *Allens Linklaters*, February 15, 2023, https://www.allens.com.au/insights-news/insights/2023/02/ChatGPT-in-law/.

[11] Faisal R. Elali and Leena N. Rachid, “AI-generated research paper fabrication and plagiarism in the scientific community,” *Patterns* 4, no. 4 (2023), https://www.sciencedirect.com/science/article/pii/S2666389923000430?via%3Dihub.

[12] Kelvin Chan, “OpenAI: ChatGPT back in Italy after meeting watchdog demands,” *Associated Press*, April 28, 2023, https://apnews.com/article/chatgpt-openai-data-privacy-italy-b9ab3d12f2b2cfe493237fd2b9675e21.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website’s Terms of Use.