Navigating GDPR Compliance in AI: A Deep Dive into OpenAI's ChatGPT — A Perspective from Multimedia Design Architecture

Alicia Colmenero-Fernandez[1]

[1]Affiliation not available

September 11, 2023

Introduction

In an era increasingly dominated by artificial intelligence, the matter of informed consent has never been more crucial. A study conducted by Ipsos indicates a significant 11-point drop in internet trust since 2019[1]. Particularly in the European Union, there is growing concern about the handling of personal data. This article aims to shed light on the ways in which AI platforms, like OpenAI's ChatGPT, fall short of meeting key guidelines established by the European Union's General Data Protection Regulation (GDPR).

Utilizing data from Enforcement Tracker, we present a graph illustrating the distribution of GDPR fines across various sectors. The Media, Telecoms, and Broadcasting sectors are particularly noteworthy, both for the number of violations and the scale of the fines imposed, signaling serious continuos non-compliance .

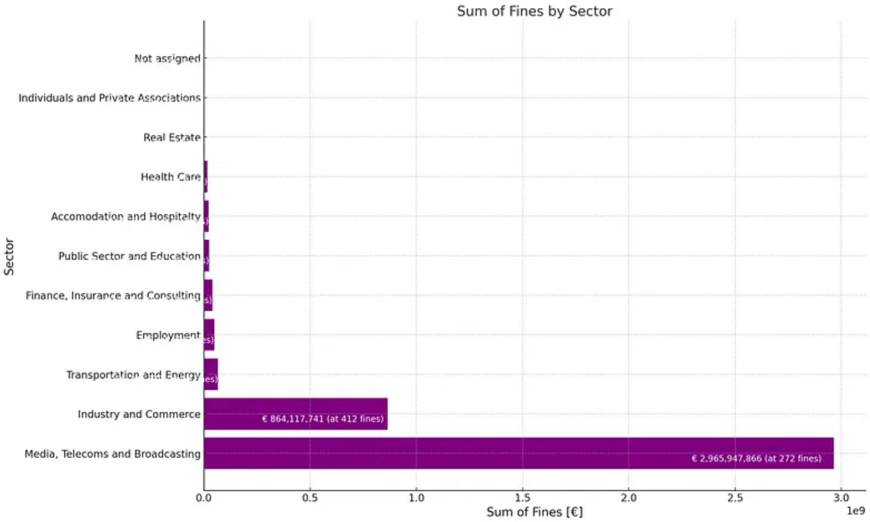


Figure 1: Sum of fines by sectors

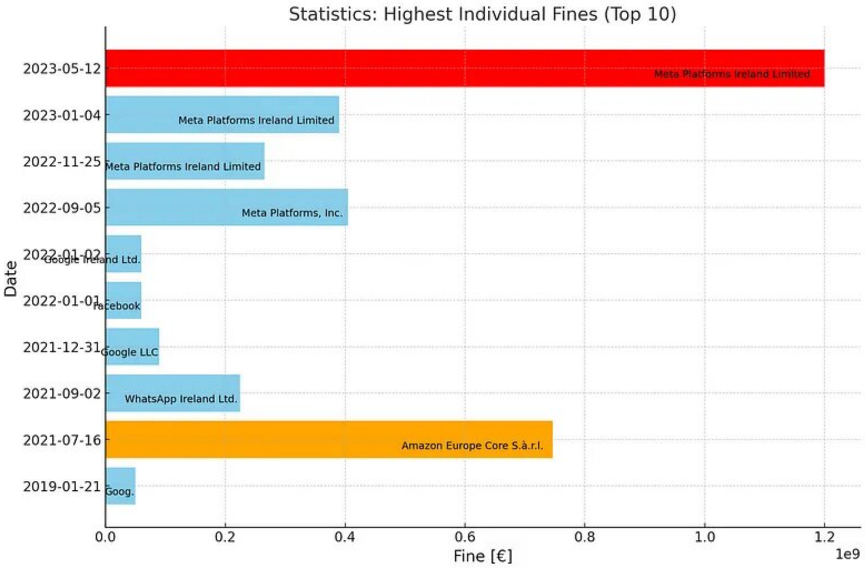


Figure 2: Statistics: Hightest Individual Fines (Top 10)

1. The Hidden Dangers of Opt-Out and Implied Consent in Data Harvesting

Risk: Steep Fines for Inadequate Consent on Personal Data Processing

When you register for the ChatGPT platform, the system is configured by default to harvest data from your conversations to enhance its algorithms. This setup shifts the burden onto you to actively opt out, a tactic that flies in the face of GDPR guidelines.

According to Articles 7.2 and 4(11) of the GDPR, genuine consent must be a "free, specific, informed, and unambiguous indication of the data subject's wishes" — a bar that opt-out strategies woefully fail to clear.

Article 4.11 EU *GDPR* : *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a* ***clear affirmative action****, signifies agreement to the processing of personal data relating to him or her; [2]*

Better Practices: Embrace an Explicit Opt-In Model for User Autonomy

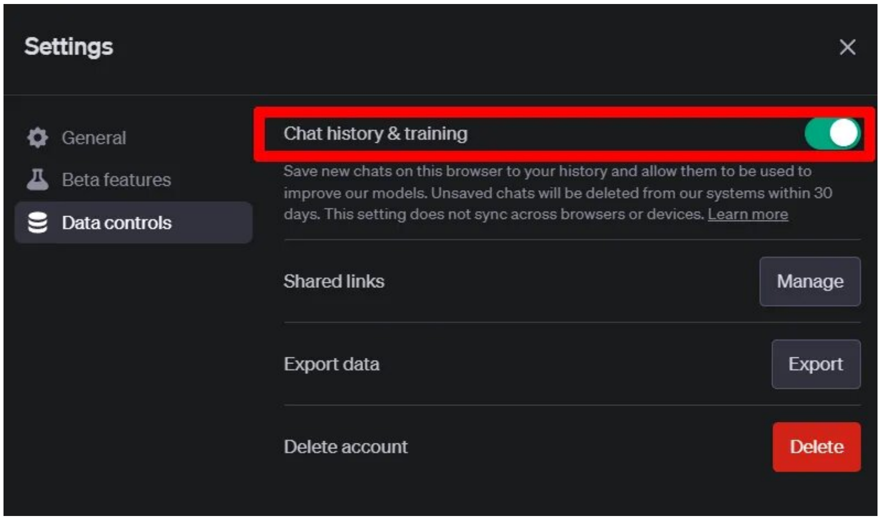
The platform ought to be upfront with users about its data collection protocols, offering them the liberty to choose whether their conversational data will be included in the dataset or not. Transitioning to an explicit opt-in model would bring the platform into greater harmony with GDPR requirements, which stipulate that consent must be free, specific, informed, and unambiguous.

From a design standpoint, adopting an explicit opt-in model is more than just a legal obligation — it's a cornerstone of a positive user experience. Users deserve to know, in no uncertain terms and plain language, what data is being gathered and for what purposes. A well-crafted consent form can make this process transparent and user-friendly, effectively ticking the boxes for both GDPR compliance and sound design principles.

2. The Flaw in Bundled Consents: Muddled Choices and Hidden Implications

Risk: Non-Compliance with Articles 7.2 of the GDPR

On the ChatGPT platform, a single toggle in the settings controls both your chat history and the use of your data for AI training. Deactivating this button not only stop future conversation from contributing to model training but also erases your chat history . However, what it doesn't make clear is that your past conversations can still be used for model training unless you navigate through additional layers to explicitly opt out.



Chat history & training ●

Save new chats on this browser to your history and allow them to be used to improve our models. Unsaved chats will be deleted from our systems within 30 days. This setting does not sync across browsers or devices. Learn more

Figure 3: Settings

***Article 7.2 EU** GDPR: [. . .]* If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.*[2]*

Best Practices: Separate and Visible Consent Options

To align with GDPR guidelines, these consent options should be unbundled and made distinct. A transparent and easily accessible setting should allow users to opt in or out of each feature independently.

User-Friendly Revocation Mechanisms

Moreover, when a user chooses to delete a specific conversation, the implications — both in terms of model training and data storage — should be clearly stated. Additionally, users should be provided with a straightforward path to opt out of having any of their past conversations used for model training.

3. Data Retention: A Dubious Policy at Odds with GDPR

Risk: Penalties for Violating GDPR and LOPDGDD Principles, Including Data Minimization and Purpose Limitation

The ChatGPT platform holds onto your information for 30 days, even after you've opted out of data training. This policy not only raises ethical questions but also appears to contradict Article 17 of the GDPR, which confers the "right to erasure."

(Platform) If I disable history, does the setting apply to all my conversations, or can I choose specific conversations to enable it for? While history is disabled, new chats will be deleted from our systems within 30 days – and reviewed only when needed to monitor for abuse – and won't be used for model training. Existing conversations will still be saved and may be used for model training if you have not opted out.*[3]*

Article 17. EU GPRD: " The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay [. . .] ".*[2]*

Best Practices: A Clear Path to Immediate Data Deletion

Given the GDPR's stringent conditions for data retention, the platform's 30-day policy raises compliance issues. Unless the platform can prove a compelling legal justification that aligns with GDPR exceptions, an immediate data erasure option should be made available and clearly marked within user settings.

4. Obstacles to Seamless Rights Exercise: The Syncing Snare

Risk: Non-Compliance with Articles 25 and 7.3 of the GDPR

The process of withdrawing your consent should be straightforward. However, the platform's settings don't sync across devices, forcing you to opt out on each device separately. This complicates matters and runs afoul of Articles 25 and 7.3 of the GDPR, which mandate that withdrawing consent should be as easy as giving it.

(PLATFORM) Does this functionality sync between web and mobile devices? *This setting does not sync across browsers or devices. You will have to enable it in each device.*

Article 25.2 EU GDPR: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*[2]*

Article 7.3 EU GDPR: The data subject shall have the right **to withdraw his or her consent at any time** . The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall **be informed** thereof. It shall be as easy to withdraw as to give consent.*[2]*

Best Practices: Streamline Consent Across Devices

The user experience should be consistent across all devices. When consent is withdrawn on one device, this choice should be universally applied to all other platforms. This is not just a hallmark of good design but is also in line with GDPR's Articles 25 and 7.3, which call for an uncomplicated withdrawal process.

5. The Maze of Consent: How Complexity Undercuts Transparency

The Hurdles in Opting Out

Withdrawing your consent on the platform is far from straightforward. To fully opt out, you must navigate through two separate links and fill out a form. The initial deactivation button, which turns off chat history and model training, only applies to future conversations. Prior chats will continue to be used for training unless you specifically navigate to and complete an additional opt-out form. This convoluted process erodes transparency and impedes users' ability to easily withdraw consent.

Recommendations for Improvement

Simplify Consent Withdrawal

Good design often adheres to the principle of "less is more." The option to withdraw consent should be easily accessible, not hidden behind multiple layers of menus or hyperlinks. A clean interface, perhaps using progressive disclosure techniques, would make the process more user-friendly.

Enhance Transparency with Clear Information Architecture

The key to improving transparency lies in robust information architecture. Users shouldn't have to dig through a labyrinth of links to manage their data and consents. A streamlined, user-focused design can go a long way in enhancing a user's ability to control their own data.

6. The Rigidity of Rectification: An Oversight in User Data Management

Risk: Fines for Infringement of Data Subject Rights, Including Access and Rectification

One area where ChatGPT falls short in GDPR compliance is in facilitating users' right to rectify their data. Article 16 of the GDPR unequivocally states that individuals have the right to correct any inaccurate personal data about themselves.

Article 16 EU GDPR: The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*[2]*

In the ChatGPT system, your email is tethered to a unique token that identifies your activity on the platform. Currently, if you change your email — which is often linked to your phone number — the platform offers no straightforward way to update this information.

Best Practices: Enable Email Address Flexibility

Users should be able to effortlessly update their associated email addresses. Streamlining this process not only enhances user experience but also brings the platform into compliance with GDPR's Article 16, concerning the right to data rectification.

UI Note for Compliance:

"To change the email linked to your account, simply follow this link: [Link to Change Email]. The procedure is reversible and designed for utmost simplicity, aligning with Article 16 of the GDPR."

Conclusion: Charting the Path Forward

Trust in AI systems isn't just desirable — it's imperative. Both legal compliance and thoughtful design must collaborate to forge a user environment that's both safe and GDPR-compliant. As we tread deeper into the AI landscape, especially concerning biometric data collection and processing, the urgency to address these issues only amplifies.

By melding principles from multimedia design architecture with GDPR guidelines, businesses can adopt a proactive stance — effectively safeguarding user privacy without compromising on experience.

¿Qué debo hacer si creo que no se han respetado mis derechos de protección de datos personales? Acciones posibles si no se ha respetado la protección de sus datos según el Derecho de la UE, como recurrir a la...

Sources:

[1] “Trust in the Internet,” Ipsos, November 2022. *Link*

[2] “UE Reglamento General de Protección de Datos,” Privacy Regulation EU. *Link*

[3]”Data Controls FAQ,” OpenAI Help Center. *Link*