OFF THE RECORD MUSIC SERVICES GDPR REVIEW

By Esteban Miranda

March 16, 2024

CONTENTS

European Union General Data Protection Regulation 2
EU Personal Data Audit 2
Consent 2
Transparent Information 2
Data Protection Impact Assessment 3
Agreements 3
Data Protection Officer 4
EU Representative 4
Data Breach Notifications 4
Transfers 5
Conclusion 5

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

The European Union General Data Protection Regulation (GDPR)[1] is a European Union law. However, it applies to any company that makes its services or websites available to data subjects as GDPR refers to EU citizens. GDPR is a European Union data privacy law that requires companies to keep EU people's data safe. It also gives the EU people rights over their data. Off The Record Music Services must comply with GDPR since OTR stores and handles data belonging to customers in the EU. OTR also handles and stores information on EU authors who publish music using OTR. Overall, OTR must comply with GDPR regarding the data belonging to EU people. The data can range to email addresses to IP addresses. The European Union enforces the law with the help of foreign governments by mutual assistance treaties.

EU PERSONAL DATA AUDIT

OTR should conduct an information audit for all EU personal data. OTR needs to determine all data concerning EU citizens. OTR should decide if the processing of personal data is for activities related to offering goods or services. Recital 23[2] can help clarify if activities qualify as subject to the GDPR.

CONSENT

OTR should inform customers why you're processing their data. GDPR Article 6[3] goes in-depth about the lawfulness of processing, consent required for processing a subject's data, and a safe way to avoid fines. GDPR clarifies the rules for consent in Article 7.[4] Consent should be freely given, meaning EU citizens can refuse whenever they want. For every piece of information to be gathered, OTR must allow the customer to consent to or refuse each one. Consent must be specific and be made clear. The request for consent should be easy to understand with a description of the data processing that will be done. For each data type to be collected, there should be an explanation and the option to consent. There should also be consent for every single data processing type. This means that consent must be received for different reasons if data is gathered for advertising or verification. Consent must be quickly informed, meaning the data subject knows everything about OTR, what data you are collecting, and the reason for the data collection. They can freely deny consent at any time. The explanation and consent agreement should be easy to read. Consent must not be assumed, and consent should be affirmed freely, specifically informed, and easily indicated, such as in a written statement. Recital 32 states the conditions for consent.

TRANSPARENT INFORMATION

Article 12[5] describes how transparent the information and communication must be regarding all data subject information. Updating the OTR privacy policy should include clear and transparent information about the data subject on everything. The privacy notice should consist of how OTR handles and processes personal data. Articles

[1] General Data Protection Regulation

[2] Recital 23

[3] Article 6

[4] Article 7

[5] Article 12

12, 13[6], and 14[7] on GDPR provide details on creating a privacy notice that describes the importance of making everything easy to read. When collecting someone's data, it is essential to provide them with a clear and concise privacy notice. The privacy notice should be well-structured and contain specific information, including the type of data collected, how it is collected and used, how it is stored, and whether it will be used for marketing purposes. Additionally, the notice should include information about the EU citizen protection rights, any changes in the privacy policy, contact information, and details of the relevant authorities that can be contacted for further information.

DATA PROTECTION IMPACT ASSESSMENT

OTR stores customer information, names, emails, and shipping addresses. They must assess the data processing procedures to help understand the risks to improve the security and privacy of the data, which are all required under GDPR. Implementing data security methods to limit data breaches and creating a Data Protection Impact Assessment (DPIA) is required to follow GDPR. Article 35[8] states many conditions where a DPIA is required, and it is recommended that the DPIA be created for best practices for security and privacy being followed by OTR. Article 35 outlines the requirements for certain elements to follow GDPR guidelines. When assessing data processing, describe the processing operations and summarize the data you plan to process and the reasons why. It is essential to determine if it is necessary and if it serves its intended purpose. Keep sentences short and straightforward, identify the risks of EU citizen's rights and freedom when processing, gathering, and storing their data. The DPIA should address the risks, safeguards, security measures, and mechanisms to protect personal data, including EU citizens' rights and legitimate interests. DPIA should be conducted before data processing activities. UK's Information Commissioner office, which enforces the GDPR in the UK, has a DPIA template available online.[9] The document will guide you through determining whether you require a DPIA. Protecting the data is extremely important; security measures such as end-to-end encryption and cybersecurity training are a few security implementations that can help keep private data secure.

AGREEMENTS

A business that relies on third parties to process personal data, such as an email client, a cloud storage service, website software, etc. must have Data Processing Agreements. Data Processing Agreements are covered in Article 28, Section 3.[10] A Data Processing Agreement is a contract that states the rights and requirements of each party regarding the importance of the protection of personal data. OTR does not store payment information on customers or authors so there must be an agreement with third parties. GDPR data processing agreement templates also serve as a guideline and can be found from reliable sources online.[11] GDPR Article 28 Section 3 explains the eight topics that must be included in the Data Processing Agreement. In summary, the third-party commits to processing personal data only as the organization instructs in writing. Everyone handling the data must keep it confidential, and proper security measures should be in place to protect it. A third-party company cannot hire someone to handle the

[6] Article 13

[7] Article 14

[8] Article 35

[9] Sample DPIA Template

[10] Article 28

[11] Data Processing Agreement Template

work that the third party and organization agreed on. If the third-party hires someone new to handle the work the third-party and organization agreed on, a new data processing agreement must be written and signed.

DATA PROTECTION OFFICER

Many organizations hire a data protection officer if necessary. GDPR mandates organizations employ a data protection officer (DPO) under specific conditions. A DPO oversees the organization being in GDPR compliance and is an expert in data protection law and practices. They oversee adherence to GDPR independently and report directly to the organization's top management. The responsibilities of a DPO include.

- addressing inquiries from EU citizens
- educating staff on GDPR requirements
- monitoring compliance efforts
- conducting assessments
- A DPO cooperates with supervisory authorities, is the primary contact for data protection matters, and supervises compliance.

Article 38[12] provides further details on a DPO's job duties. Organizations must hire DPOs if they are public authorities, engage in large-scale monitoring, or extensively process data types. The definition of large scale depends on the number of EU citizens, data volume, and types of processing. A part-time DPO might be recommended to be safe, while a full-time DPO for OTF might not be necessary.

EU REPRESENTATIVE

Article 27[13] of the GDPR outlines more rules for organizations outside the EU that process the personal data of individuals must designate a representative within the EU. Recital 80[14] provides more information on the role of the representative. The EU representative will serve as a primary point of contact for individuals and authorities in the EU regarding data protection. The representative acts on behalf of the organization and acts as a point of contact for EU data protection authorities. The requirement applies to organizations outside the EU that offer goods or services to individuals in the EU. However, exceptions exist if the data processing is occasional, doesn’t involve large processing of sensitive data, or poses a minimal risk to EU citizens.

DATA BREACH NOTIFICATIONS

According to Article 33[15] of the GDPR, organizations must notify the supervisory authority of any personal data breach within three days of becoming aware of the incident. Notification is not necessary unless it poses a risk to individuals' rights and freedoms. It's important to note that public authorities are exempt from this requirement. The

[12] Article 38

[13] Article 27

[14] Recital 80

[15] Article 33

organization should notify the DPO after becoming aware of a personal data breach. The notification to the DPO should include details of the breach, the number of affected individuals, and data records. The name and contact details of the DPO or other point of contact where more information can be acquired should be included in the notification of the supervisory authority. The text should include a description of the breach, the measures taken to address it, and any steps taken to mitigate the effects of the breach on personal data. If certain information is available immediately then it can be provided in phases. The organization must keep records of breaches, including their details, impact, and actions to fix them. The records should enable the supervisory authority to verify compliance with Article 33. Article 34[16] outlines the communication of a personal data breach to affected individuals. The organization should inform the EU citizens if the breach risks individuals' rights and freedoms. Communication is optional for EU citizens if certain conditions are met. For example, if the controllers implemented security measures such as encrypting the affected personal data. Suppose actions have been taken to mitigate the data of the subject's rights and freedoms risk. Public announcements are allowed to inform EU citizens effectively.

TRANSFERS

Article 45[17] discusses the conditions for transferring personal data to a country outside the EU without authorization. The transfer is allowed if the European Commission has determined that the government has proper data security, which is very important. Article 45 details how the EU Commission assesses the best practices for data protection and reviews them every four years to consider new updates. The EU publishes the list of countries on its website that they have approved for adequate protection. The Data Privacy Framework[18] is recommended since it adds many benefits to following GDPR. The DPF offers a structured approach to data privacy compliance, specifically GDPR, and ensures adequate protection for data transfers, simplifying contractual arrangements and providing cost-effective solutions.

CONCLUSION

In conclusion, OTR must follow GDPR since they handle personal data belonging to EU citizens. OTR must follow the GDPR frameworks, or else it will result in a large fine, or OTR could shut down. Data audits are required to handle EU-related personal data. Consent is essential for data processing, and it should be clear when requested from EU citizens. OTR should be transparent in handling data belonging to EU citizens and respecting their privacy rights. OTR should also conduct Data Protection Impact Assessments (DPIA) to assess and prevent risks associated with the different types of data processing. Data Processing Agreements with third-party service providers are essential to follow GDPR. A DPO is recommended since they are skilled in compliance with GDPR. OTR must acquire a representative within the EU since it operates outside the EU; the representative is a point of contact for EU data protection. If a data breach occurs, OTR must notify the proper authorities and affected EU citizens within the GDPR regulations. International data transfers for OTR must follow the requirements in Article 45. OTR will successfully follow GDPR and protect the personal data of EU citizens if it follows the recommendations.

[16] Article 34

[17] Article 45

[18] Data Privacy Framework

References

Official GDPR. (2016, April 27). eur-lex.europa.eu. Retrieved March 16, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Wolford, B. (2023, September 14). *GDPR compliance checklist for US companies*. GDPR.eu. https://gdpr.eu/compliance-checklist-us-companies/