This developer name is TREND MUSIC STYLE
we are built application
Privacy Policy
Effective date: April 04, 2022
This application ("us", "we", or "our") operates the website and theThis application mobile application (the "Service").
This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data.
Our Privacy Policy for This application is managed through Free Privacy Policy.
We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions.
Information Collection And Use
We collect several different types of information for various purposes to provide and improve our Service to you.
Types of Data Collected
Personal Data
While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:
· Cookies and Usage Data
Usage Data
We may also collect information that your browser sends whenever you visit our Service or when you access the Service by or through a mobile device ("Usage Data").
This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.
When you access the Service by or through a mobile device, this Usage Data may include information such as the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.
Tracking & Cookies Data
We use cookies and similar tracking technologies to track the activity on our Service and hold certain information.
Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device.
Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Service.
You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.
Examples of Cookies we use:
· Session Cookies. We use Session Cookies to operate our Service.
· Preference Cookies. We use Preference Cookies to remember your preferences and various settings.
· Security Cookies. We use Security Cookies for security purposes.

Use of Data
This application uses the collected data for various purposes:
· To provide and maintain the Service
· To notify you about changes to our Service
· To allow you to participate in interactive features of our Service when you choose to do so
· To provide customer care and support
· To provide analysis or valuable information so that we can improve the Service
· To monitor the usage of the Service
· To detect, prevent and address technical issues
Link to privacy policy of third party service providers used by the app

Google Play Services
AdMob
Facebook

Log Data

I want to inform you that whenever you use my Service, in a case of an error in the app I collect data and information (through third party products) on your phone called Log Data. This Log Data may include information such as your device Internet Protocol (“IP”) address, device name, operating system version, the configuration of the app when utilizing my Service, the time and date of your use of the Service, and other statistics.

GDPR
The **General Data Protection Regulation (GDPR)** is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises (SMEs).

We created this website to serve as a resource for SME owners and managers to address specific challenges they may face. While it is not a substitute for legal advice, it may help you to understand where to focus your GDPR compliance efforts. We also offer tips on **privacy tools** and how to mitigate risks. As the GDPR continues to be interpreted, we’ll keep you up to date on evolving best practices.

If you've found this page — "what is the GDPR?" — chances are you're looking for a crash course. Maybe you haven't even found the document itself yet (tip: **here's the full regulation**). Maybe you don't have time to read the whole thing. This page is for you. In this article, we try to demystify the GDPR and, we hope, make it less overwhelming for SMEs concerned about GDPR compliance.

History of the GDPR

The right to privacy is part of the 1950 **European Convention on Human Rights**, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence." From this basis, the European Union has sought to ensure the protection of this right through legislation.

As technology progressed and the Internet was invented, the EU recognized the need for modern protections. So in 1995 it passed the European Data Protection Directive, establishing minimum data privacy and security standards, upon which each member state based its own implementing law. But already the Internet was morphing into the data Hoover it is today. In 1994, the **first banner ad** appeared online. In 2000, a majority of financial institutions offered online banking. In 2006, Facebook opened to the public. In 2011, a Google user sued the company for scanning her emails. Two months after that, Europe's data protection authority declared the EU needed "a comprehensive approach on personal data protection" and work began to update the 1995 directive.

The GDPR entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant.

Scope, penalties, and key definitions

First, if you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you even if you're not in the EU. We talk more about this **in another article**.

Second, the fines for violating the GDPR are very high. There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages. We also talk **more about GDPR fines**.

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. **Pseudonymous** data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.

Data subject — The person whose data is processed. These are your customers or site visitors.

Data controller — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. These could include cloud servers, like **Google Drive**, **Proton Drive**, or **Microsoft OneDrive,** or email service providers, like **Proton Mail**.

What the GDPR says about…

For the rest of this article, we will briefly explain all the key regulatory points of the GDPR.

Data protection principles

If you process data, you have to do so according to seven protection and accountability principles outlined in **Article 5.1-2**:

1. Lawfulness, fairness and transparency — Processing must be lawful, fair, and transparent to the data subject.
2. Purpose limitation — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. Data minimization — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. Accuracy — You must keep personal data accurate and up to date.

5. Storage limitation — You may only store personally identifying data for as long as necessary for the specified purpose.
6. Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Accountability

The GDPR says data controllers have to be able to demonstrate they are GDPR compliant. And this isn't something you can do after the fact: If you think you are compliant with the GDPR but can't show how, then you're not GDPR compliant. Among the ways you can do this:

- Designate data protection responsibilities to your team.
- Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.
- Train your staff and implement technical and organizational security measures.
- Have Data Processing Agreement contracts in place with third parties you contract to process data for you.
- Appoint a Data Protection Officer (though not all organizations need one — more on that in **this article**).

Data security

You're required to handle data securely by implementing "**appropriate technical and organizational measures**."

Technical measures mean anything from requiring your employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.

Organizational measures are things like staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it.

If you have a data breach, you have 72 hours to tell the data subjects or face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker.)

Data protection by design and by default

From now on, everything you do in your organization must, "by design and by default," consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity. The GDPR covers this principle in **Article 25**.

Suppose, for example, you're launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

When you're allowed to process data

Article 6 lists the instances in which it's legal to process person data. Don't even think about touching somebody's personal data — don't collect it, don't store it, don't sell it to advertisers — unless you can justify it with one of the following:

1. The data subject gave you specific, unambiguous consent to process the data. (e.g. They've opted in to your marketing email list.)
2. Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. (e.g. You need to do a background check before leasing property to a prospective tenant.)
3. You need to process it to comply with a legal obligation of yours. (e.g. You receive an order from the court in your jurisdiction.)
4. You need to process the data to save somebody's life. (e.g. Well, you'll probably know when this one applies.)
5. Processing is necessary to perform a task in the public interest or to carry out some official function. (e.g. You're a private garbage collection company.)
6. You have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data. (It's difficult to give an example here because there are a variety of factors you'll need to consider for your case. The UK Information Commissioner's Office provides helpful guidance **here**.)

Once you've determined the lawful basis for your data processing, you need to document this basis and notify the data subject (transparency!). And if you decide

later to change your justification, you need to have a good reason, document this reason, and notify the data subject.

Consent

There are strict new rules about what constitutes **consent from a data subject** to process their information.

- Consent must be “freely given, specific, informed and unambiguous.”
- Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”
- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can’t simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent.

Data Protection Officers

Contrary to popular belief, not every data controller or processor needs to appoint a **Data Protection Officer (DPO)**. There are three conditions under which you are required to appoint a DPO:

1. You are a public authority other than a court acting in a judicial capacity.
2. Your core activities require you to monitor people systematically and regularly on a large scale. (e.g. You’re Google.)
3. Your core activities are large-scale processing of special categories of data listed under **Article 9** of the GDPR or data relating to criminal convictions and offenses mentioned in **Article 10**. (e.g. You’re a medical office.)

You could also choose to designate a DPO even if you aren’t required to. There are benefits to having someone in this role. Their basic tasks involve understanding the GDPR and how it applies to the organization, advising people in the organization about their responsibilities, conducting data protection trainings, conducting audits and monitoring GDPR compliance, and serving as a liaison with regulators.

We go in depth about the DPO role **in another article**.

People’s privacy rights

You are a data controller and/or a data processor. But as a person who uses the Internet, you’re also a data subject. The GDPR recognizes a litany of new **privacy rights for data subjects**, which aim to give individuals more control over the data they loan to organizations. As an organization, it’s important to understand these rights to ensure you are GDPR compliant.

Below is a rundown of data subjects’ privacy rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Conclusion

We’ve just covered all the major points of the GDPR in a little over 2,000 words. The **regulation itself** (not including the accompanying directives) is 88 pages. If you’re affected by the GDPR, we strongly recommend that someone in your organization reads it and that you consult an attorney to ensure you are GDPR compliant.

Transfer Of Data
Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.
If you are located outside Turkey and choose to provide information to us, please note that we transfer the data, including Personal Data, to Turkey and process it there.
Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.
This application will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.
Disclosure Of Data
Legal Requirements
This application may disclose your Personal Data in the good faith belief that such action is necessary to:

- To comply with a legal obligation
- To protect and defend the rights or property of This application
- To prevent or investigate possible wrongdoing in connection with the Service
- To protect the personal safety of users of the Service or the public
- To protect against legal liability

Security Of Data

The security of your data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

Service Providers

We may employ third party companies and individuals to facilitate our Service ("Service Providers"), to provide the Service on our behalf, to perform Service-related services or to assist us in analyzing how our Service is used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

Links To Other Sites

Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Children's Privacy

Our Service does not address anyone under the age of 18 ("Children").

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your Children has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

Changes To This Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.you can send e-mail :musicshopapp@gmail.com