GDPR Policy for BotG

What is GDPR?

GDPR stands for General Data Protection Regulation. A new law enforced by EU to protect end user's personal data. This law enforce several aspect of data security. Here we want to give a guideline how we protect your data, what is our responsibility and what is your responsibility. We strongly suggest you read all our documentation or other article about GDPR and take decision whether you want to use our application or not. We are not responsible for any negligence or fault on data protection on your side or any third party side. Take your time to read documentation and act wisely, stay safe.

Definition of Personal Data

Any data owned by an individual is his or her personal data. It could be someone's name, image, email address, physical address, social media post, location, computer IP address etc. The ownership of user's personal data is absolute. That means wherever and however the data is saved it belongs to the user solely. The data collector or data user (facebook, youtube) cannot show, save, share or perform any other activity with user's personal data without user's explicit or implicit permission. If an user gives permission to use his or her data on specific type of action (data storing, data viewing etc) then it can be used by the admin of the application. To visualize this consider a hypothetical situation. You post a status on social media. Here you have given the implicit permission to show the post to your public or private contacts. Application admin is not responsible for any abusive comment to your post made by your contacts. This means that if you made your data public then it is your responsibility. But application admin do hold responsible for any data sharing with third party. If any data is shared it must be said explicitly in advance. So we see the how data uploading and showing depends on both app admin and user. Further details you will get upon reading the full documentation.

Responsibility of Developer

The safeguard of user personal data on application back end is the responsibility of developer. Developer is responsible for how the user data (name, telephone no. email etc) and other info (like logs of user interaction with application) is stored on database and server. We will describe in detail how the data you submit directly (name, email etc.) and indirectly (browser name, computer IP etc.) are saved on database and server. Once any data uploaded to server the security of data depends on security of server and sometimes the admin of application. User will be notified about all the temporary (cookie and session) and permanent (data saved to database) data saving. User will get the option of all his or her personal data erasing permanently upon account deletion or service cancellation. We assure you that we do not keep logs of user activity and any other backdoor to extract user data. Sometime cpanel access and other credential of app admin is needed by the developer to support and maintaining of the application for short time before the application goes full online. We strongly recommend to app admin to change these credential after the job get done. Developer cannot be held responsible for any credential leak on this ground. Developer also cannot be held responsible for any unwilling security glitch on the application. After all, data shared online always has the risk of getting leaked. So we strongly suggest not to share any data that can compromise you any other individual.

Responsibility of Application Admin

Application Admin has unrestricted access the user personal data. Admin can access to database, server logs and any other info on admin's reach. Application admin can see and copy the data saved

on database and server. App admin can share user's personal data to third parties. How the user's data is used must be announced by the app admin explicitly before user registration. The admin should not allow anyone to extract data openly or under disguise of survey, fill the form or any other means. The app admin enjoys most privilege on application. So admin has the highest responsibility of safekeeping of user's personal data.

User's Responsibility

It's all depends on user. If user do not submit data then there will be no data breach. But this is not an option. The top most priority of user is to read all the documentation from both app developer and app admin then submit the data. Safe keeping of user's own credential is sole responsibility of user. Password and username may be encrypted on database but a dictionary word or too predictable password for a specific user can give easily access to user's account to hacker. Change your credential on any suspicious activity by unauthorized person or in case of you share your credential to other for some inevitable reason. Always think before submit.

Our Action on GDPR

- Collect as less data as possible. Tell the user necessity or collecting specific data.
- Enforce https
- Destroy all session and cookies after logout.
- Do not track user activity for commercial purpose.
- Tell users of any logs that saves computer ip and location.
- Clear terms and condition.
- Inform user about any data sharing with third parties.
- Create clear policies about data breaches.
- Delete data on cancelling subscription or account deletion.
- Patch web vulnerabilities.

Supported GDPR Features

Adios, Application: Once you cancel your subscription or delete account we give you option to delete all your data existing or related to your account. Note that, this action is irreversible. The moment you say yes to delete all your data will be erased from the database and server forever. You can back up data before delete in case of re subscribe or re-register.

Secrecy is my right: We encrypt most of your personal data on database. If any bad things occur (data breach) then the hacker will get encrypted hash not your personal on plain text. So your secrecy will intact even in case of data breach. Note that, some data cannot be encrypted because we need to show it upon login to account (like username). We will hide all your personal data as much as possible.

No cookie and session saving: We will give option to save or do not save cookie and session. Even if you save cookie and session these will be destroyed after logout. We strongly suggest you not save your credential in browser. Please memorize your credential or use tools like lastpass to manage your credential.

Destroy footprints: We do not save or track any of your activity for any commercial purpose. We may store your login time or IP for security purpose only. When you delete your account every single piece of your data will be deleted from server.

Social engineering is bad: We do not record any of your personal activity on the application. Recording user's personal activity, analyzing it and try to sell a product or motivating user to pursue a certain thought upon analyzed data is becoming a malpractice. We do not do such things.

Notify me: Get notified about all your activity relating to your account (account creation, password change) by email. We suggest you to change your credential if any unusual things occur.

Policy Update notification: You will get notified on any privacy policy or disclaimer updates. Read your email regarding to this matter and decide your action. Feel free to consult on this matter.

Connect without worry: We enforced HTTPS everywhere. Data sniffing is not possible on this case. Even possible, the sniffer will get encrypted hash. So feel safe to use our application.

No data collecting: We do not collect any data of user. No backdoor, No hidden option to collect data. Once the application is uploaded to server even we cannot enter to application without app admin password. So do not worry about any hidden data leak.

Data breach policy: We implement all the security to store your data carefully on database (data encryption, MySQLi, SQL injection prevention, input checking etc.). But we do not take any responsibility of data breaches from server. Because it is total responsibility of app admin and server admin to secure your data from breaching. Any weak or too predictable password of app admin or server admin could compromise database. Any inherent fault on database config can give away the database (MongoDB security fault). Any security flaw on server can lead to data leaking. Please contact your app admin on this regard.