simplelists

Your GDPR email compliance checklist

Simplelists want to help make sure that your organisation remains compliant with GDPR requirements. So, we've put together a checklist of 10 essential steps to follow when sending emails.

1. Obtain consent: Before adding anyone to your email list, make sure you have explicit consent. Provide a clear and easy-to-understand way for users to opt-in, and that documents their consent.
2. Double opt-in: Implement a double opt-in process to confirm subscribers' consent. This typically involves sending an email with a confirmation link that the user must click to verify their subscription.
3. Privacy policy: Ensure that your privacy policy is easily accessible and transparent. It should provide details of how you collect, store, and process personal data. Plus, let users know how they can exercise their rights under the GDPR.
4. Data minimisation: Only collect and process the personal data necessary for the specific purpose you have stated. Avoid requesting or storing excessive amounts of data that you don't need for your email campaigns.
5. Data storage: Store personal data securely and limit access to only those who need it for the specific purpose you have stated. Implement strong security measures and protocols to protect data from unauthorized access and data breaches.
6. Data retention: Be clear about how long you will retain personal data in your system. Set a reasonable retention period and delete data when it's no longer needed for the purpose you have stated.
7. Data subject rights: Inform your email subscribers about their rights under the GDPR, including the right to access, rectify, erase, restrict processing, and data portability. Provide an easy process for them to exercise their rights.

8. Unsubscribe mechanism: Include an easy-to-find and straightforward unsubscribe link in every email you send. Make sure users can easily opt out of receiving future communications, and promptly process their requests.
9. Data protection officer (DPO): If your organization is required to do so under the GDPR, appoint a DPO. The DPO is responsible for overseeing data protection activities and ensuring GDPR compliance.
10. Data breach notifications: Develop a plan for handling data breaches and reporting to the relevant authorities within 72 hours of the breach notification. You will also need to notify affected individuals without delay if the breach poses a high risk to their rights and freedoms.

By following these steps, you can make sure that your email communications are GDPR-compliant and protect the personal data of your subscribers. Implementing these practices will not only help you avoid potential fines but also fosters trust and transparency with your audience.

See how Simplelists can help you comply with GDPR at https://www.simplelists.com