



Listing out compliance tasks

A

I just moved to a B2B health tech product that enables doctors to accept patient appointments online, share digital prescriptions & send out automated alerts to remind them when a visit is due. My boss wants me to ensure we are GDPR compliant. Can you explain what GDPR is in my context and what steps I should take?



Sure, here is a summary of how you can ensure GDPR compliance for your B2B health tech platform that enables doctors to accept patient appointments online, share digital prescriptions & send out automated alerts to remind them when a visit is due:

- Conduct a data protection impact assessment (DPIA) to identify and assess any potential risks to individuals' personal data that may arise from your product. This will help you to identify any areas where you need to improve your data protection practices.
- Appoint a Data Protection Officer (DPO) who will be responsible for ensuring that your company complies with GDPR and for providing advice and guidance on data protection.
- Ensure that you have a clear and up-to-date privacy policy that sets out how you collect, use, and store personal data, including patient information such as name, date of birth, medical history, and contact information. This policy should be easily accessible to patients and other users of your product.
- Obtain explicit, informed consent from patients before collecting, using, or sharing their personal data. This can be done through an online form or an in-person agreement.
- Implement appropriate technical and organizational measures to protect personal data from unauthorized access, accidental loss, or destruction. This includes using encryption, firewalls, and intrusion detection systems to protect patient data.
- Regularly review and update your data protection practices to ensure that they remain compliant with GDPR.
- Keep records of all data processing activities under GDPR and be ready to provide evidence of your compliance if required by supervisory authorities.

It is important to note that GDPR is a complex regulation and it's important to seek legal advice to ensure that you're fully compliant with the regulation.