HIGHSIDE

GDPR & HighSide

What you need to know about the GDPR and how HighSide helps you ensure compliance

GDPR governs the processing, storage and use of personal data for citizens of the European Union (and the UK). As most people are aware, it's a regulation that has sharp penalties for non-compliance and governs just about all use of customer data. One of the reasons GDPR presents such a challenge to many businesses is that it takes a very wide view on what is considered personal data. For example, organisations now need to treat an IP or cookie information the same way they would treat someone's passport number or national identity number. In the best of times, this causes serious headaches for security and compliance teams, but with Covid induced remote work the new-normal, things have changed once again.

The GDPR leaves a lot to individual interpretation, making it even harder (and more costly) on the business to ensure compliance. "Reasonable protection for personal data doesn't really define much.

GDPR is relevant to your organization if you have...

- A presence in an EU country (and the UK)
- No presence in the EU (or the UK) but customers / personal data of EU (and UK) residents
- More than 250 employees
- Fewer than 250 employees but... well, basically processes personal data of EU (and UK) citizens

The GDPR focus on two main "actors", controllers and processors. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

If you are a controller, you are responsible for complying with the UK GDPR – you must be able to demonstrate compliance with the data protection principles, and take appropriate technical and organisational measures to ensure your processing is carried out in line with the UK GDPR.

Controllers (you) are responsible for most of the GDPR compliance regulation. Not only are you on the hook for how your employees use and handle personal data, but you are on the hook to make sure your provider has the right controls in place to meet the GDPR. Because of the imbalance in responsibility between controllers and processors, choosing a platform that will enable you to store and share your GDPR controlled data, in a secure and compliant manner is a challenge.

Simplify GDPR Compliance With HighSide

You have enough to worry about when it comes to GDPR and personal data protection, don't let your data sharing and collaboration provider be one of those worries.

HighSide lets you communicate internally and with external third parties through group and individual chat, voice, video & screen sharing - while also enabling you to save, share, and use sensitive & GDPR regulated data, files, folders, documents and more through one, secure platform. Leveraging HighSide's revolutionary distributed encryption protocol and secure SaaS cloud, completely E2E encrypted data comes standard... as does GDPR compliance.

Let's take a look at a handful of the articles from the GDPR and dissect how HighSide makes your life significantly easier →

Article 6. Lawful basis of processing

"The controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: appropriate safeguards, which may include encryption or pseudonymisation."

Because HighSide is E2E encrypted, your data is never available to HighSide or any other third party. Organizations that are using HighSide's platform don't have to worry about how GDPR protected data is used, stored or shared by HighSide, eliminating a big stress for compliance teams. HighSide gives organizations the ability to collaborate, where appropriate, with comfort knowing any activity involving personal data is within compliance.

Article 25. Data protection by design and by default

"The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures."

HighSide eliminates the need for compliance and security teams to determine technical requirements for the processing of data for storage or sharing. The E2E encrypted nature of the HighSide platform lets authorized users access personal data to complete their job without worrying about the security or safety of that information. Additionally, HighSide provides a full compliance suite that records immutable event logs ensuring a complete picture of who, what, when, and where data was accessed.

The centrally managed HighSide platform gives admins full control over data access, even as granular as setting acceptable physical locations for data usage. For example, many HighSide customers lock employees from accessing personal data unless they are in an approved location such as their home office or the corporate office. This simple (and patented) capability ensures you not only know what device and what user accessed personal data, but that you know where it was accessed from. Eliminate the risk of poor security hygiene (like viewing personal data on a train, in a coffee shop or at a pub) with HighSide's built-in access control systems.

Article 32. Security of Processing

"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data"

HighSide's E2E encrypted service delivers out-of-the-box compliance with Article 32 of the GDPR. Unlike other collaboration platforms and file sharing services, customers don't need to pay more for a secure version of the service nor do they need to think about how to match risk level with security controls. HighSide ensures that all data is encrypted, all the time - in fact, HighSide isn't technically the processor of the data since data is never decrypted nor can it be.

Article 34. Communication of a personal data breach to the data subject

"The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;"

GDPR provides strict guidance on how personal data affected in a data breach or leak must be communicated, and how notifications to those individuals must be handled. Without exception, notifying customers of a data breach drives a drop in trust and has a direct impact on revenues, public market valuation, and brand loyalty (impacting future revenues). When personal data is stored in the HighSide cloud, there is a zero percent chance of a data breach (due to the E2E encrypted nature of the platform). With HighSide, organizations avoid one of the biggest impacts to their operations, data breach, and the notification requirements that come with it.

*HighSide is the modern **collaboration platform** for **security conscious teams**. HighSide's all-in-one business productivity app delivers security, compliance and productivity through decentralized crytopgrahy and E2E encryption - see for yourself at highside.io*