



Enabling Our Customers to be GDPR Compliant



GDPR

Data Privacy and Protection has been one of most critical topic for customers ever since world of digitalization took over.

GDPR, the EU data protection law that came in effect on 25 May 2018 helped in institutionalization of data privacy and protection in organizations. It applies to the processing of personal data carried out by organizations operating within the EU or to organizations outside the EU that have data on EU citizens.

We at Comport, leave no stone unturned to make sure that our customers get all the support to be compliant with GDPR.



Comport is completely GDPR compliant and our platform gives options to customers for being compliant with GDPR by handling Personally Identifiable Information (PIIs) appropriately and taking care of users right and consent management



Why you should care about GDPR ?

GDPR considers the protection of personal data as a fundamental right for EU citizens. The impact of GDPR is significant as it affects any business that collects data in Europe (whether they are based in Europe or not).

GDPR puts a greater responsibility on individuals and organizations whose businesses involve collection of personal data and requires those businesses to give individuals greater visibility into, and control over the data they provide to those businesses.

There is very high fines and penalties of up to €20Mn or 4% of global annual turnover, whichever is greater, may be levied on organizations who fail to meet GDPR obligations



What has Comport Done for GDPR

We understand that you put heavy reliance on us when you store and process sensitive and personal information on our platform. To take this customer trust to next level Comport has made sure not only to be GDPR compliant but also aspires to take additional steps to make the platform more secure. Following are few of the initiatives that we have taken:



Data Security

Data protection and security are primary consideration for us and as requirement of GDPR. We are covering every aspect of security data across people, process and technology stack.

We get security assessments of our platforms done regular from independent parties to make sure we comply with requirements but secure applications.

We are also working towards ISO 27001 certification as part of our security program. Contact us for more details on security of our application and processes



Security & Privacy Incidents

Putting robust set of security and privacy controls in place, certainly reduces the probability of incidents. However, any level of security systems can not completely safeguard against security incidents or data breaches, we have detailed security incident policies and procedures in place and frequently review these procedures. We take all possible steps as per defined processes to keep our customers informed for any such unforeseen incident in future, in-line with GDPR requirements. Our robust security monitoring system helps us in early identification of any such potential incidents.



Data Privacy Notice

We updated our Privacy Policy to reflect our commitment for Data Protection of our customer's PII/sensitive data and to address the evolving needs of our all our customers, both self serve and Enterprise. Transparency and accuracy are our key drivers in making these changes, and we believe the more succinct and easily navigable policy which applies to all our services, will be useful to our customers

Our Privacy Notice is available on our website. The objective of privacy notice is to inform our customer about all personal information that we record. It sets out what information we collect from you and the conditions under which we may process any information that we collect from you, or that you provide to us. It covers information that could identify you ("personal information") and information that could not. In the context of the law and this notice, "process" means collect, store, transfer, use or otherwise act on information.



International Data Transfers

In addition to the initiatives highlighted above, we are aware that many of our customers with EU users and EU affiliates would prefer that their data be hosted in the EU, notwithstanding the methods for lawful data transfer that we provide. To ensure to meet international data transfer compliances, we use the following safeguards with respect to data transferred outside the European Union:

- The processor is within the same corporate group as our business or organization and abides by the same binding corporate rules regarding data processing.
- The data protection clauses in our contracts with data processors include transfer clauses written by or approved by a supervisory authority in the European Union
- We comply with a code of conduct approved by a supervisory authority in the European Union
- We are GDPR compliant under compliant requirements & mechanism as provided for in the GDPR Law
- Both our organization and the processor are public authorities between whom there is either a legally binding agreement or administrative arrangements



Data Accuracy & Minimization

Privacy by design and privacy by default are an intrinsic part of our product planning and development. One example of how we can help customers address their obligations under GDPR while using Compport is through the admin control panel. Through the control panel your account administrator can edit, export, or delete any data collected from their employees/ users.



Data Retention

We have company-wide data retention policies and procedure implemented to ensure your data is stored with us no longer than is necessary for the purpose(s) or legal requirements.

All personal and sensitive data of data subject are adequate, relevant and stored in a secure area/ database. Data outside Compport environment is communicated through a secure channel using encryption.

a. Data accuracy: We always check the accuracy of the data before processing it. If data subject's data/record is identified as inaccurate or insufficient then data is corrected and confirmed with Data Subject for accuracy.

b. Data update: Once a data update request is received from the Data subject, DPO or delegate verifies the requestor/data subject, and post verification designated Compport team member updates the data in timely manner that is within 72 hours. Post update, the confirmation is shared with Data subject/requestor.

c. Data storage: Data storage is recording of data/records in the database. All data/records stored on IT infrastructure owned and/or leased by Compport are encrypted. Physical data records will be stored in areas with restricted access. Access to stored data shall be restricted to authorized users only



Data Recording Security and Storage



DPO

We have appointed a Data Protection Officer and they are responsible for all matters related to GDPR. The DPO can be contacted through dpo@compport.com

Contact Us



+971-508189912, +971-553998819
+91-8130096266, +91-8130268058



dpo@compport.com



www.compport.com



Disclaimer: This awareness note is not to be leveraged in construing legal advice or representative of our interpretation of GDPR or privacy laws. The intent of this document is to help our customers understand our approach to GDPR in practical terms. In order to get any legal advice in the related topic we strongly recommend customers to get an independent legal counsel.