







Questionmark and the GDPR

The General Data Protection Regulation (GDPR) is the European Union (EU) privacy law about processing personal data of individuals in the EU. If you are delivering assessments in the EU, you will need to comply with the GDPR even if your organization is based outside of the EU. Questionmark itself will be compliant with the GDPR, and this data sheet explains some of the ways we will help customers using Questionmark OnDemand and Questionmark OnPremise be compliant.

| GDPR Compliance Measure | Questionmark follows? | How Questionmark helps: |
|--|---|--|
| Only process personal data on your instructions |  | Questionmark is a data processor under the GDPR. Personal data is only processed for operating the service and is erased after you stop using the service. See Questionmark's privacy policy for more information. |
| Inform of and get an approval of subcontractors/sub-processors |  | We disclose the small number of sub-processors we use, and if they change, we follow the GDPR procedure to obtain general authorization from customers. |
| Contract meets GDPR needs |  | All our standard contracts are GDPR compliant, and we'll try to accommodate any other contractual needs you may have. |
| Strong security measures to protect personal data |  | Questionmark is ISO 27001 certified. See www.questionmark.com/trust for details on our security. |

| | | |
|---|---|---|
| <p>Personal data outside the EU is protected</p> |  | <p>Questionmark has EU model clauses in place with sub-processors and will enter into EU model clauses with customers.</p> |
| <p>Help ensure personal data is accurate</p> |  | <p>Under the GDPR, customers as data controllers need to ensure personal data is accurate. For assessments, it's crucial that results are not only accurate but also valid, reliable and defensible. Questionmark products contain tools that empower customers to meet these objectives.</p> |
| <p>Deal appropriately with sensitive data</p> |  | <p>Questionmark doesn't require or default entering any sensitive or special categories of data, but can hold it if required.</p> |
| <p>Provide information to aid transparency notices to test-takers</p> |  | <p>See here for personal information assessments typically capture and reach out to us with any questions you have.</p> |
| <p>Support for writing a Data Protection Impact Assessment (DPIA)</p> |  | <p>Questionmark has a template available to help customers write DPIAs.</p> |
| <p>Personal data can be erased</p> |  | <p>Questionmark lets you erase data with the ability to permanently delete assessment results when required. Please raise any erasure needs with technical support.</p> |
| <p>Help answer access requests from data subjects</p> |  | <p>Questionmark has a comprehensive range of reports which allow you to respond to subject access requests.</p> |

| | | |
|--|---|--|
| <p>Inform promptly in event of a data breach</p> |  | <p>Questionmark has a regularly-tested incident response plan and puts customers on our breach notification list for rapid communication in the event of a breach.</p> |
| <p>Expert, reliable data processor</p> |  | <p>Questionmark’s legal counsel (Jamie Armstrong (FIP; CIPP/E/US/C; CIPM; CIPT) leads Questionmark data protection and is our DPO. Several other members of the team hold current IAPP privacy certifications. We train all our staff on data protection and the GDPR.</p> |