Morressier Platform Security and Privacy FAQ

Is Morressier GDPR compliant?	Yes. Morressier's main entity is based in Germany and complies fully with GDPR. A Data Processing Addendum (DPA) forms part of all our contracts and details information on data protection and privacy.
Where can I find more information on Data Privacy at Morressier?	Our latest privacy policy can be found at: www.morressier.com/company/privacy-policy
Where can I find the list of Morressier sub-processors?	In keeping with GDPR compliance we maintain a list of all sub-processors as part of our Record of Processing Activities. An up-to-date list is available upon request which includes information on the specific data that is processed, for what purpose, and by which sub processor.
Where do we store customer data?	Morressier hosts data in different locations across mainland Europe. Our main data centers are in the Frankfurt, Germany region. Backup and recovery sites are in St. Ghislain, Belgium and Eemshaven, Netherlands.
Who has access to customer data?	We safeguard customer data by restricting access to Morressier employees solely for the purpose of delivering our services.
How is customer data protected at rest?	Customer data stored on Morressier systems is protected by AES 256, a military-grade encryption algorithm.
How do we ensure protection of data transfers over the Internet?	The data flow between customer endpoints and Morressier occurs over TLS 1.2 & 1.3 encrypted connections, which provide server authentication and data encryption. Data is never exchanged in cleartext.

Do you support different roles and permissions on your platform?	The platform has a built-in Role-Based Access Control (RBAC). Client accounts with Administrator privileges can assign permissions on a granular level to each user or group. Critical actions and access is audited and logged.
How do you protect your platform from malicious attacks?	Morressier applies layers of protection at different levels including DDoS (Distributed Denial of Service) protection, Web Application Firewalls, and network firewalls to limit traffic.
Do we keep backups of customer data and how are they protected?	Yes, depending on the system we have either continuous backups that allow point in time recovery or 30 minute backups intervals. We keep 7 days of backups at different locations and regularly test restore procedures. Backups are stored encrypted.
How long do you keep backups of customer data stored?	We keep backups of customer data stored for 28 days.
What password requirements are in place to protect customer's data?	Customers can use their existing SSO Identity provider for authentication to Morressier. Some examples include Azure AD, Okta, Google, and on-prem Active Directory. Any system that supports SAML 2.0 or OpenID Connect (OIDC) protocols can be linked with Morressier for authentication. New user accounts can be provisioned via SSO and roles and permissions are also able to linked via SSO mechanisms.
Do you conduct regular penetration testing of your application?	Penetration tests covering the API and web application are performed by a third-party reputable security testing company. Tests are conducted annually or when there's a significant change in our architecture.
Do you allow customers to undertake their own security testing?	Yes, we allow enterprise customers to undertake their own security testing given that Morressier is notified in advance and results are disclosed. There may be additional costs involved to provide the necessary access and support. We handle these requests on a case by case basis.
How do we process credit card data?	We do not collect or process any credit card data.