GO ANYWHERE®
Managed File Transfer

DATASHEET *(Cybersecurity)*

Meeting GDPR Requirements with GoAnywhere MFT

The General Data Protection Regulation (GDPR) is a regulation approved by the European Parliament. It applies to all organizations that handle and process EU citizens' data, regardless of whether they're located in the European Union or not. Failure to meet GDPR requirements can result in huge penalties: 4% of annual global turnover (revenue) or €20 million, whichever is greater.

The GDPR was created to replace the Data Protection Directive, which has been used in the EU for over 20 years. There are several key changes, also knows as rights, introduced to the GDPR that organizations must address; thinking about them now is critical to successful compliance. For some companies, GDPR rights may require excessive work and planning if the requested processes aren't already implemented.

GoAnywhere MFT is a managed file transfer solution that runs on any system. It can help you meet GDPR compliance standards, while saving you time and money in other business areas. It can also eliminate the custom programming and scripting normally required to transfer data and improve the security and quality of those transfers.

Address Your Security and Compliance Needs

GoAnywhere MFT helps organizations meet GDPR requirements by providing an auditable solution with secure file transfers, secure mail, and data encryption. The benefits of GoAnywhere for security and compliance needs include:

- Encryption of data in transit and at rest
- Detailed audit logs for reporting
- Secure connections for the transmission of sensitive data
- Strong encryption key management that stays in your control
- Centralized control and management of file transfers
- Role-based administration and permissions
- Secure mail module for sending files using email with HTTPS download links

Organizations must be in compliance with many GDPR requirements, and the new regulation gives IT and security teams a lot to consider. By implementing robust solutions, businesses can meet these requirements—while also building a strong foundation for future security needs.

PROTECT YOUR DATA WITH ENCRYPTION

The General Data Protection Regulation requires the personal data of all EU citizens to be secured. Organizations must be able to provide a "reasonable level of data protection and privacy" upon request, no matter if it's located on-premises, remotely, or in the cloud.

In order to comply with the GDPR, companies should implement encryption into their security policies. GoAnywhere MFT offers several popular technologies to help businesses secure sensitive data. Use encrypted folders, OpenPGP, SSL, SSH, ZIP with AES, and an integrated key manager to ensure your business and clients are always protected.

GoAnywhere Helps You Meet GDPR Requirements

GoAnywhere MFT can help organizations address certain GDPR requirements through several key features, including data encryption, integrity checks of successful file transfers, secure forms for subject consent, and detailed audit trails.

	GDPR Required Standards	Corresponding GoAnywhere Feature
Required Standards	**Requirement: Article 5.1(e), 5.2** Personal data shall be processed in a manner that ensures appropriate security of the personal data. The controller shall be responsible for, and be able to demonstrate compliance with, the security.	GoAnywhere has several popular encryption technologies, including AES 256-bit encrypted folders that protect files at rest, ZIP with AES for compressing and encrypting files, OpenPGP compliant encryption that addresses the privacy and integrity of data, and SSH/SSL security for encrypting file transfers. With GoAnywhere, you remain in control of the security and data at all times. Use detailed reports of file transfer activity, user statistics, and completed jobs to prove compliance with article 5.
	Requirement: Article 7, 8 Individuals must give consent to have their personal data collected and used. Consent must be separable from other written agreements.	Personalize and send your consent forms through GoAnywhere's Secure Forms module. Designate a form as public and send users access with a link, then collect consent and receive files (document scans, form signatures, and so on) as encrypted attachments. All submission history, including date stamps and user responses, is logged for auditing and reports.
	Requirement: Article 15, 20 EU citizens may request a copy of data and request to transfer personal data from company to company upon request.	Use GoAnywhere's Secure Forms module to create a data request form. When a user requests a copy of their data, GoAnywhere can encrypt and send the requested information through GoAnywhere's password-protected Secure Mail. This entire process can be completely automated with project workflows, and Secure Mail can be sent from within GoAnywhere's browser interface or via Microsoft Outlook.
	Requirement: Article 25 Organizations must be able to provide a reasonable level of data protection and privacy.	GoAnywhere MFT provides data protection and privacy through user roles, allowing the admin to limit who can view or process information. It also provides encryption for data in transit and at rest.
	Requirement: Article 30 Records of processing activities must be maintained, including the type of data processed and the purposes for which it's used.	GoAnywhere allows you to store and track detailed audit information. It generates comprehensive audit logs of all file transfer and administrator activity, which you can schedule on a regular basis, then search and view through browser-based administration or a PDF report.
	Requirement: Article 32 Controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	Many GoAnywhere features ensure a stringent level of security for personal data, both in transit and at rest. Use GoAnywhere's encryption technologies, encryption key management, and admin user roles to implement a solid security strategy for your business.
	Requirement: Article 39.1(b), 39.2 A Data Protection Officer shall be able to monitor compliance with the GDPR regulation (assigning responsibilities, related audits).	GoAnywhere's Admin Roles allow you to assign GoAnywhere functions to authorized users. Admin User Roles contain Auditor and Security Officer roles immediately, giving you the ability to assign a Data Protection Officer access to whatever they need for monitoring purposes. GoAnywhere MFT is also managed from a single, central location, giving you control over everything without needing multiple logins, products, or unrelated add-ons.

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.