Fields Auto Group Compliance

Service Provider Risk Assessment

Questionnaire requested by **FIELDS AUTO GROUP**

Meghan Gibbons	GOTO COMMUNICATIONS, INC.	3.18.2026
Name of Person Completing This Questionnaire	**Service Provider Name**	**Date Completed**

1. Are you an employee or authorized representative of this vendor/company? Indicate the Person's Name in the comments.	☒ Yes ☐ No ☐ N/A	Person's Name: Meghan Gibbons Manager, RFP Team
2. Does your company offer software applications as part of its services?	☒ Yes ☐ No ☐ N/A	
3. Is client data encrypted at rest and in transit? If not, why not?	☒ Yes ☐ No ☐ N/A	Further details on encryption outlined within our GoTo Connect TOMs.
4. Has your company experienced a data breach in the past 12 months that affected customers' personal information?	☐ Yes ☒ No ☐ N/A	
5. Does your company have insurance coverage for a data breach that may involve our customer information that your company acquires while doing business with us?	☒ Yes ☐ No ☐ N/A	Certificate of Insurance can be provided upon request.
6. Does your company require security awareness training for all employees? If so, please answer how often it is provided in the comments section.	☒ Yes ☐ No ☐ N/A	Security Training Frequency: GoTo maintains a comprehensive awareness program to ensure employees handle personal and confidential data responsibly and in compliance with applicable laws and industry standards. All new hires, contractors, and interns receive privacy and security training during onboarding. Employees complete quarterly awareness training that addresses current risks, including AI security considerations. We also provide secure coding training for developers to strengthen product security. Annual campaigns and role-specific training reinforce our commitment to meeting regulatory requirements such as HIPAA and PCI, supporting audit readiness and internal maturity goals.

7. Does your company monitor for the effectiveness of employee security training by testing your users with simulated attacks?	☒ Yes ☐ No ☐ N/A	
8. Does your company have a process for restricting access to customer files on a need-to-know basis?	☒ Yes ☐ No ☐ N/A	GoTo implements robust logical access control procedures to mitigate the risk of unauthorized access and data loss. Access to GoTo systems, applications, networks, and devices is granted to employees based on the 'principle of least privilege,' ensuring that users only have the minimum level of access necessary for their roles. User privileges are segregated based on functional roles (role-based access control) and environments, utilizing segregation of duties controls, processes, and procedures. To maintain the highest level of security, these logical access controls are reviewed quarterly, ensuring they remain effective and up-to-date in preventing unauthorized access.
9. Do you have a written information security program?	☒ Yes ☐ No ☐ N/A	GoTo maintains a comprehensive set of security policies and procedures that align with business goals, compliance and privacy programs, and overall corporate governance. These policies and procedures are reviewed and updated at least annually to support GoTo's security and business objectives, adapt to changes in applicable laws, and meet industry standards.
10. Does your company conduct annual risk assessments that assess electronic, physical, and administrative information safeguards?	☒ Yes ☐ No ☐ N/A	GoTo follows a structured, control-based approach to manage risk. We identify threats through assessments like threat modeling and compliance reviews, then apply safeguards such as access controls, encryption, and continuous monitoring. Security priorities are set based on risk impact, ensuring consistent, risk-informed decisions that strengthen resilience and protect our brand.

11. Does your company have systems in place to securely dispose of documents that have personal identifiable information on them?	☒ Yes ☐ No ☐ N/A	GoTo disposes of confidential information to meet our confidentiality commitments and system requirements. We have policies and procedures that encompass: • Locates and removes or redacts specified confidential information as required • Regularly and systematically destroys, erases, or makes anonymous confidential information that is no longer required for the purposes identified in its confidentiality commitments or system requirements. • Clear devices prior to repurposing or destroying • Disposal of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies • Documents the disposal of confidential information
12. Does your company have systems in place to restrict access to files/documents containing customers personal information to those with proper authorization?	☒ Yes ☐ No ☐ N/A	GoTo implements robust logical access control procedures to mitigate the risk of unauthorized access and data loss. Access to GoTo systems, applications, networks, and devices is granted to employees based on the 'principle of least privilege,' ensuring that users only have the minimum level of access necessary for their roles. User privileges are segregated based on functional roles (role-based access control) and environments, utilizing segregation of duties controls, processes, and procedures. To maintain the highest level of security, these logical access controls are reviewed quarterly, ensuring they remain effective and up-to-date in preventing unauthorized access.
13. Does your company have due diligence processes and procedures for vetting subcontractors, including	☒ Yes ☐ No ☐ N/A	GoTo follows a structured procurement process before engaging any third-party vendor that handles Customer Content or

having them sign processing agreements that are compliant with applicable federal and state laws?		sensitive data. This process includes: • Reviewing the vendor's security and privacy practices • Obtaining and evaluating compliance documentation when required by regulation or contractual obligations • Ensuring written agreements meet GoTo's privacy and security standards Our Finance, Legal, Privacy, GRC, and Security teams collaborate to verify mandatory data handling and contractual requirements. Agreements include compliance with applicable laws and, where required, Data Processing Agreements (DPAs) covering regulations such as GDPR, CCPA, LGPD, and HIPAA. For HIPAA-related services, GoTo also executes Business Associate Agreements (BAAs) with relevant vendors. Security addenda with appropriate controls are applied to vendors as needed.
14. Has your company performed penetration testing of its systems within the past 12 months?	☒ Yes ☐ No ☐ N/A	Testing is done on an annual cadence.
15. Has your company conducted a vulnerability assessment of your systems within the past 6 months?	☒ Yes ☐ No ☐ N/A	GoTo employs a comprehensive vulnerability management approach to safeguard the security and integrity of our systems and data. Our process involves systematically identifying, assessing, prioritizing, and remediating vulnerabilities to maintain a robust security posture. We utilize a variety of security tools, platforms, and external sources to detect vulnerabilities, followed by thorough reviews and rigorous testing to address any identified issues. By consolidating, correlating and interpreting findings from diverse sources, we implement effective security measures that ensure our products remain secure and reliable for our customers. GoTo's Security

		Automation Framework Engine (SAFE) is vital for remediation, accurately classifying and assigning vulnerabilities to ensure a sustainable reduction over time. We continuously scan our cloud environments for vulnerabilities, sort them based on priority, and report them to engineering and management via SAFE, enabling prompt resolution.
16. Does your company maintain end-of-life or unsupported operating systems or software? If so, are these systems used to manage or maintain customer data?	☐ Yes ☒ No ☐ N/A	
17. Does your company regularly patch or update systems and third-party software and monitor for noncompliance?	☒ Yes ☐ No ☐ N/A	GoTo's patch management strategy is designed to minimize the technical and business impact of known vulnerabilities through a series of well-defined steps that leverages Microsoft Azure Update Manager. Patches are deployed in phases, starting with a small test group and gradually expanding to encompass all systems. This phased approach helps identify and resolve issues early, reducing risk and maintaining system availability. Zero-day patches are given higher priority and expedited timelines to address critical vulnerabilities promptly. Systems are rebooted as necessary to ensure patches take effect. The strategy includes monitoring patch levels, obtaining patches from trusted sources, assessing risks, testing patches, prioritizing deployment, reporting on deployment status, and managing failed deployments with rollback procedures.
18. Does your company have a written incident response plan in the event of a security breach?	☒ Yes ☐ No ☐ N/A	GoTo's Security Operations Center (SOC) is dedicated to detecting and responding to security events with precision and efficiency. Our SOC employs advanced security sensors and analysis systems to identify potential issues. To ensure a swift and effective response, we have

		developed comprehensive incident response procedures, including a documented Incident Response Plan that is tested annually. This Incident Response Plan is meticulously aligned with GoTo's critical communication processes, policies, and standard operating procedures. It is designed to identify, manage, and resolve suspected or identified security events across our systems and services. The plan outlines clear mechanisms for employees to report suspected security events and provides detailed escalation paths to follow when necessary. To enhance our threat detection capabilities, GoTo utilizes a Security Information and Event Management (SIEM) tool. This tool helps correlate security events, enabling us to identify suspicious activities more effectively. Suspected events are documented and escalated as appropriate via standardized event tickets and are triaged based on their criticality. This robust approach ensures that we maintain a secure environment and respond promptly to any potential threats.
19. Does your company require users to create complex passwords with 9 characters or greater?	☒ Yes ☐ No ☐ N/A	All user-level and system-level passwords at GoTo must conform to our password requirements: the length of the minimum characters required (16 characters) which is double the character length of the standard 8 characters. With that, our employees all should have a very secure strong password (with 3 of 4 complexity rules). Thus, we do not require our employees to change their password. Additionally, we also require MFA so the combination of a strong password and MFA provides very secure access controls to our environment.

		IT distributes the userID and password together in a secure encrypted email to our users. Administrative user passwords that are NOT managed through group memberships or other authentication processes must be a randomly generate string of at least 20 characters using upper and lower case letters, numbers, and special characters. First-time passwords for new users, and reset passwords for existing users, should be set to a unique value for each user and changed after first use User accounts are temporarily locked-out after not more than five invalid access attempts. Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. System/session idle time out features have been set to 15 minutes or less. Passwords are protected with strong cryptography during transmission and storage.
20. Does your company prohibit shared logins?	☒ Yes ☐ No ☐ N/A	
20. Does your company prohibit shared logins?	☒ Yes ☐ No ☐ N/A	
22. Do you have an account lockout policy?	☒ Yes ☐ No ☐ N/A	

3/18/2026	Meghan Gibbons	Manager, RFP Analysts
Date	**Signature of Authorized Agent of Service Provider**	**Title**