Fields Auto Group Compliance

Service Provider Risk Assessment

Questionnaire requested by **ENTER FIELDS LOCATIONS HERE**

Thomas Bennett	Epsilon	5/12/2025
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.	X☑ Yes ☐ No ☐ N/A	Person's Name:
2. Does your company offer software applications as part of its services?	☐ Yes ☐ No ☐ N/A	Yes.
3. Is client data encrypted at rest and in transit? If not, why not?	☑ Yes ☐ No ☐ N/A	TLS v1.2 in transit; AES 256 at rest
4. Has your company experienced a data breach in the past 12 months that affected customers' personal information?	☐ Yes ☑ No ☐ N/A	No confirmed breaches in past 12 months
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	Yes. Epsilon maintains required coverage for Cybersecurity incidents
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	Yes. All employees are required to complete Security Training upon hire and annually thereafter
7. Does your company monitor for the effectiveness of employee security training by testing your users with simulated attacks?	☑ Yes ☐ No ☐ N/A	Yes. Phishing exercises are regularly conducted
8. Does your company have a process for restricting access to customer files on a need-to-know basis?	☑ Yes ☐ No ☐ N/A	Yes. Access is granted based on Least Privilege and Need to Know
9. Do you have a written information security program?	☑ Yes ☐ No ☐ N/A	Yes. The Global Security Office (GSO) maintains a Comprehensive set of Information Security policies aligned with the requirements of the ISO 27001 Security Standard. The GSO is responsible for the management, review and updates of security policies.

		Approvals are executed by the Chief Executive Officer.
10. Does your company conduct annual risk assessments that assess electronic, physical, and administrative information safeguards?	☑ Yes ☐ No ☐ N/A	Yes. Formal risk assessments are conducted annually to identify any security risks through security testing, reviewing security policies, exception management, incident analysis, monitoring of technology services and feedback provided by interested parties
11. Does your company have systems in place to securely dispose of documents that have personal identifiable information on them?	☑ Yes ☐ No ☐ N/A	Yes. Epsilon uses a vetted and experienced vendor for media destruction. A certificate of secure shredding is provided when completed. Epsilon's policy requires wiping, degaussing and physical destruction of obsolete equipment and media, such as tape and disk drives. The drives are degaussed and shredded if we are recycling the hardware. A certificate of destruction is provided for any destruction performed.
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	Yes. Access to client data is severely restricted to Epsilon users who have a clearly demonstrated need to know based on role.Direct access to the DB is restricted to a few vital Epsilon employees with a highly demonstrated need for access. Access is managed by a limited set of Epsilon resources. Any change to provisioning or decommissioning of user accounts is requested in accordance with the documented Access Control Policy.

13. Does your company have due diligence processes and procedures for vetting subcontractors, including having them sign processing agreements that are compliant with applicable federal and state laws?	☑ Yes ☐ No ☐ N/A	Yes. All suppliers/subcontractors are assessed in accordance with the Security Risk Management Program and contracts are in place
14. Has your company performed penetration testing of its systems within the past 12 months?	☑ Yes ☐ No ☐ N/A	Yes. Epsilon has a documented vulnerability management procedure in place that defines methods of identifying, reporting and managing vulnerabilities affecting the Epsilon network. Scans of Network perimeter, devices and critical infrastructure systems are regularly performed; annual network Penetration Testing is conducted annually by accredited third party. Identified vulnerabilities are communicated to relevant stakeholders and closed according to their priority.
15. Has your company conducted a vulnerability assessment of your systems within the past 6 months?	☑ Yes ☐ No ☐ N/A	Yes. Epsilon is ISO 27001 Certified and undergoes annual SSAE 18 SOC 1, 2 and 3 audits and assessed as an approved PCI DSS Level One Service Provider. Epsilon also conducts internal audits and Risk Assessments of contracted external third party firms/vendors to ensure compliance with both corporate and relevant industry standard control objectives.
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	No. End of Life or unsupported systems/software is prohibited
17. Does your company regularly patch or update systems and third-party software and monitor for noncompliance?	☑ Yes ☐ No ☐ N/A	Yes. Patching may vary based on the criticality of the patch. Best practices include monthly patching windows with an

		exception process supporting immediate patching base on the risk.
18. Does your company have a written incident response plan in the event of a security breach?	☑ Yes ☐ No ☐ N/A	Yes. Epsilon has in place a detailed Incident Response Team (IRT), Policy and Plan. The Incident Response Team lead the investigation with Legal's guidance to ensure that the appropriate evidence is properly identified and maintained, and that the proper chain of custody occurs. The IR Policy and Plan are based on 24 x 7 x 365 response availability and on the principles of Preparation, Identification, Assessment, Containment, Eradication, Recovery, Follow-up and Post Mortem.
19. Does your company require users to create complex passwords with 9 characters or greater?	☐ Yes ☐ No ☑ N/A	At least 8 characters. At least one upper case ii. At least one lower case iii. At least one non-alphanumeric character . At least one number (0 through 9) c. Not the user's ID or name d. Only characters available on a standard English (U.S.) keyboard e. Changed every 120 days f. Account locked out after 5 unsuccessful password attempts g. Password history set to 10, which means the last 10 passwords cannot be reused
20. Does your company prohibit shared logins?	☑ Yes ☐ No ☐ N/A	Yes
20. Does your company prohibit shared logins?	☑ Yes ☐ No ☐ N/A	Yes
22. Do you have an account lockout policy?	☑ Yes ☐ No ☐ N/A	Yes; after 5 failed attempts

5/12/2025 *Thomas Bennett* Sr Account Director

Date **Signature of Authorized Agent of Service Provider** **Title**