General Data Protection Regulation ("GDPR") Policy Statement

Shift4 Payments, LLC, (Shift4) is a leader in secure payment processing solutions, powering the top point-of-sale and software providers across numerous verticals, including food and beverage, hospitality, lodging, gaming, retail, and e-commerce. This includes the company's Harbortouch, Restaurant Manager, POSItouch, and Future POS brands, as well as over 300 additional software integrations in virtually every industry. With eight offices across the U.S. and Europe, 7,000 sales partners, and two state-of-the-art Data centers, the company securely processes over 1 billion transactions annually for nearly 200,000 businesses, representing over $100 billion in payments each year.

Shift4 operates as an Independent Sales Organization (ISO) reselling American Express, Discover Card, JCB, MasterCard, and Visa credit card processing services under a West America Bank sponsorship. Shift4 makes contracts with and processes credit card transactions on behalf of Merchants. Shift4 offers Merchants Credit Card transaction point-to-point encryption, tokenization, and other value-add security services under the security frameworks of the Payment Card Industry (PCI).

Shift4 is also an active participant of the EU-U.S. Privacy Shield Framework.

The PCI Security Standards Council (PCI SSC) is a global, open body forum whose purpose is to develop, enhance, disseminate, and assist with the understanding of security standards and payment account security. The Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and globally facilitate the broad adoption of consistent data security measures. The PCI DSS provides a baseline of technical and operational requirements designed to protect account data. The PCI DSS applies to ***all*** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. The PCI DSS also applies to ***all*** other entities that store, process or transmit cardholder data and/or sensitive authentication Data (SAD). All other PCI security standards are based on and/or correlate to the PCI DSS.

Based on the premise that some Shift4 Merchants have relationships with EU Citizens (Data Subjects), Shift4 declares itself a Processor under the EU Data Protection Laws and the General Data Protection Regulation.

1. The type of Personal Data that Shift4 processes is systematically restricted to PCI-defined cardholder data, which is credit card:

    1.1. Primary Account Number (PAN)

    1.2. Cardholder Name

    1.3. Expiration Date

    1.4. Service Code

2. **Definitions Under the GDPR:**

2.1. EU. The European Union.

2.2. Data Protection Laws. EU Data Protection Laws and to the extent applicable, the data protection laws of any other country.

2.3. GDPR. EU General Data Protection Regulation 2016/679.

2.4. Data Subject. The natural person who is identified or identifiable by Personal Data.

2.5. Consent. Freely given, specific, informed, and explicit consent by statement or action signifying agreement to the processing of their Personal Data.

2.6. Data Controller. The entity that determines the purposes, conditions and means of the processing of Personal Data. For the purposes of this GDPR policy, the term Merchant will be used interchangeably.

2.7. Data Erasure. Also known as the right to be forgotten, it entitles the Data Subject to have the Data controller erase his/her Personal Data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

2.8. Data Portability. The requirement for Data Controllers to provide the Data Subject with a copy of his or her data in a format that allows for easy use with another Data Controller.

2.9. Data Processor. The entity that processes Personal Data on behalf of the Data Controller.

2.10. Data Protection Authority. National authorities tasked with the protection of Data and privacy as well as monitoring and enforcement of the data protection regulations within the EU.

2.11. Data Protection Officer. An expert on data security and privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR. The Data Protection Officer of Shift4 Payments, LLC is Stephen Ames, Vice President of Compliance.

2.12. Encrypted Data. Personal Data that is protected through technological measures to ensure that the Data is only accessible/readable by those with specified access.

2.13. Enterprise. Any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

2.14. Filing System. Any specific set of Personal Data that is accessible according to specific criteria, or able to be queried.

2.15. Personal Data. Any information related to a natural person or Data Subject, that can be used to directly or indirectly identify the person. For the purposes of this GDPR policy, the term "cardholder data" will be used interchangeably.

2.16. Personal Data Breach. A breach of security leading to the accidental or unlawful disclosure, destruction, misuse, etc. of Personal Data.

2.17. Process or Processing. Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as: collection, recording, organization, structuring, storage, adaptation or alteration, retrievals, consultation, use, disclosure or transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.18. Recipient. Entity to which the Personal Data are disclosed.

2.19. Right to be Forgotten. Also known as data erasure. It entitles the Data Subject to have the Data Controller erase his/her Personal Data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

3. **Data Protection Principles.** Shift4 processes, stores, and transmits cardholder data in compliance with the internationally recognized PCI Data Security Standard (DSS). Shift4's internal security controls are assessed annually by an independent, PCI Qualified Security Assessor, and have been consistently judged far above the minimum standards called out in the PCI DSS. Shift4 is committed to processing Cardholder Data in accordance with its responsibilities under the GDPR and with the contracts it makes with Merchants. Article 5 of the GDPR requires that Personal Data shall be:

3.1. Processed lawfully, fairly and in a transparent manner in relation to individuals. Shift4 processes, stores, and transmits cardholder data as defined by and in compliance with the internationally recognized Payment Card Industry Data Security Standard (PCI DSS) and the terms, requirements, and definitions contained within the Merchant services agreements Shift4 executes with its Merchants. Other than authorization and settlements services, cardholder data is never used for any other purpose and is never disclosed to or shared with third parties not directly involved with payment processing or acquiring.

3.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. Shift4 processes, stores, and transmits cardholder data in compliance with the Merchant services agreements Shift4 executes with its Merchants. Shift4's systems process all cardholder data exactly the same way and the process will always involve disclosure to third parties to provide authorization and settlement services to Merchants.

3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Shift4 processes, stores, and transmits cardholder data in compliance with the Merchant services agreements Shift4 executes with its Merchants.

3.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. If a transaction can't be processed accurately it will be systematically rejected. The cardholder data Shift4 stores is encrypted and static in nature.

3.5. Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. The retention period of cardholder data stored by Shift4 is set by merchants, but can be no longer than two years. If the merchant does not select a retention period Shift4 will systematically purge stored cardholder data after two years.

4. **General provisions.** This policy applies to all Cardholder Data processed by Shift4.

4.1. The Shift4 Data Protection Officer (DPO) shall own responsibility for Shift4's ongoing compliance with this policy.

4.2. The DPO – Stephen Ames – can be contacted by emailing GDPR@Shift4.com.

4.3. This GDPR policy shall be reviewed at least annually.

5. **Lawful, Fair, Transparent, and Compliant Processing.**

5.1. To ensure its processing of Personal Data is lawful, fair, transparent, and compliant, Shift4 will process, store, and transmit Personal Data in compliance with credit card brand rules and the PCI DSS.

5.2. The Data Processing systems shall be reviewed at least annually by internal staff, as well as by an independent Qualified Security Assessor (QSA) company under PCI rules.

5.3. Data Subjects have the right to access their Personal Data. Data Subjects must initiate this process with the Merchant that initially collected, or directed the collection of the cardholder data. As Data Controllers, Merchants have the ability to provide Data Subjects access to their Personal Data via Shift4's online systems, which is limited to PCI DSS defined cardholder data. Merchants needing assistance from Shift4 to correct, amend, or delete cardholder data shall notify Shift4 via Certified US Mail or signature courier service. Cardholder data will not be retrievable if the date of the request is past its retirement date.

6. **Contractual and Lawful Purposes.**

6.1. All Personal Data processed by Shift4 shall be done under the terms of the Merchant (or Data Controller) services agreement and the GDPR Processor Addendum it consummates with Merchants and in compliance with the EU Data Protection Laws and the PCI DSS. Unless a separate agreement is entered into with the Merchant with respect to GDPR, Shift4 shall operate under the terms of the GDPR Processor Addendum.

6.2. The Merchant (or Data Controller) shall notify Shift4 that it has relationships with EU Data Subjects under the GDPR and also submit its Data Controller Policy Statement indicating Shift4 as a Personal Data Processor. The Merchant shall also be searchable in the database maintained by the Information Commissioner's Office (ICO).

6.3. Once the conditions in 6.2 above are met, a GDPR Processor Addendum from Shift4 may be consummated. As such the terms of the Contract and the GDPR Processor Addendum are in full force unless otherwise agreed by Merchant (or Data Controller) and Shift4

6.4. Where consent is relied upon as a lawful basis for processing Personal Data, evidence of opt-in consent shall be maintained by the Merchant (Data Controller).

6.5. The option for EU Data Subjects to revoke their consent shall be made available by the Merchant (or Data Controller). The Merchant shall notify Shift4 in writing via Certified US Mail or courier service when EU Data Subjects revoke consent and assistance is required.

7. **Data Minimization.**

7.1. Shift4 shall ensure that Personal Data are adequate, relevant, and limited to what is contractually required in normal credit card transaction processing.

7.2. The PCI DSS and the credit card brands prescribe the minimum Personal Data necessary to process a credit card transaction.

8. **Accuracy**

8.1. Shift4 shall take commercially reasonable steps to ensure Personal Data is accurate.

8.2. When processing is complete, payment card transactions are static in nature and do not change, but can be reused by the Merchant for recurring payments by EU Data Subjects.

9. **Archiving/removal.** The retention period for Personal Data maintained by Shift4 is individually set by Merchants, but is systematically limited to two years at which time Shift4's system will automatically purge Personal Data. Once purged, the Personal Data is not recoverable.

10. **Security**

    10.1. Shift4 shall ensure that Personal Data is securely processed, stored, and transmitted under the credit card brand rules and in compliance with the PCI DSS. This includes the use of security technologies and measures such as firewalls and strong encryption.

    10.2. Access to Personal Data is strictly limited to personnel with a need-to-know.

    10.3. Security controls are in place to prevent unauthorized sharing or viewing of Personal Data.

    10.4. Personal Data back-up and disaster recovery processes are in place to ensure data availability.

11. **Breach.** In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, Shift4 shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the affected EU Data Subject Merchants and the ICO.

12. **Notification Information**. If any third party wishes to contact Shift4 with respect to this policy, please adhere to the following:

    General Information: GDPR@Shift4.com

    Requests for Action: Shift4 Payments, LLC
    1491 Center Crossing Road
    Las Vegas, NV 89144
    Attn: Data Protection Officer