Data Processing Addendum

For Services provided in the EU and the UK by the Shift4 group of entities

THIS DATA PROCESSING ADDENDUM ("**DPA**"), including its Annexes, forms an integral part of the Agreement between the Client and Processor (both as defined below and, each a "**Party**" and collectively the "**Parties**") which relates to the Services provided by Processor to Client and defines the data processing relationship between the Parties. This Addendum sets out the terms, requirements, and conditions on which Personal Data is processed when providing Services under the Agreement and shall supersede any other data processing addendums or documents previously signed, unless specifically agreed otherwise between the Parties. This Addendum contains the mandatory clauses required by Article 28(3) of the GDPR for contracts between Controllers and Processors.

1. Definitions

The following capitalised terms shall bear the meaning ascribed thereto. Definitions of capitalised terms that are not defined in this Addendum can be found in other parts of the respective Agreement.

"**ADC**" means Account Data Compromise, an occurrence that results, directly or indirectly, in the unauthorised access to or disclosure of account data, or the unauthorised manipulation of account data controls, such as account usage and spending limits, as defined by the Card Schemes.

"**Addendum**" means this addendum in its entirety, including any privacy related schedules and annexes as may added to the Agreement from time to time.

"**Adequacy Decision**" means the decision made by the European Commission or by the UK Information Commissioner's Office that a third country, territory, specific sector in a third country or an international organisation offers levels of data protection that are essentially equivalent to that within the European Union or the United Kingdom. An adequacy decision permits a cross-border data transfer outside the European Union or the United Kingdom, or onward transfer from or to a party outside the European Union or the United Kingdom without further authorisation.

"**Agreement**" means any of the agreements between the Parties, as may be applicable:

- Acquiring Agreement between Shift4 Limited or Shift4 Payments UK Limited and Merchant (either directly or via a Provider, as defined in the agreement)
- Local Payment Methods (LPM) Agreement between Shift4 Limited or Shift4 Payments UK Limited and Merchant
- Payment Facilitator Agreement between Shift4 Limited or Shift4 Payments UK Limited and Payment Facilitator
- Reseller Agreement between Shift4 Technology Limited and Reseller
- SkyTab Agreement between Shift4 Solutions Limited and Merchant
- Payment Gateway Agreement between Shift4 Technology Limited and Client

"**Client**" means the legal entity receiving Services from Processor, and as defined in the relevant Agreement: Client, Merchant, Payment Facilitator, or Reseller. The use of the term Client in this DPA is for convenience only and it shall refer to either Client, Merchant, Payment Facilitator, or Reseller unless specifically stated as otherwise.

"**Client Data**" means Personal Data of Client's management or UBOs or contacts provided to Shift4 by, or on behalf of, Client, including via Provider and/or Third Party Operator (as defined in the relevant Agreement), or to which Shift4 obtains access solely as a result of, or in connection with, the provision of the Services.

"**Controller**" means the entity which determines the purposes and means of the processing of Personal Data, and for the purposes of this Addendum it means Client.

"**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

"**Data Protection Laws**" means (i) the GDPR; (ii) Maltese Data Protection Laws; (iii) United Kingdom Data Protection Laws; (iv) other legislation and regulatory requirements in force from time to time which apply to each of the Parties respectively relating to the use of Personal Data; and (v) the guidance and codes of practice issued by the relevant data protection or Supervisory Authority and applicable to either Party, in each case as may be amended, supplemented, or replaced from time to time.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates. Data Subjects include: (i) Client's Cardholders, as defined in the Agreement or buyers of Client's goods and/or services; and (ii) Client's employees, directors, UBO's, shareholders, and any other individuals on whom Shift4 performs AML and KYC checks, as defined in the relevant Agreement. For clarification purposes, where Shift4 processes Personal Data to perform AML and KYC checks, it acts as a Controller.

"**EEA**" means the European Economic Area, which for the purpose of this DPA shall also include the United Kingdom.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of Personal Data and on the free movement of such data as in force as amended, replaced, or superseded from time to time, including any laws implementing or supplementing the GDPR, including as implemented under the laws of the United Kingdom.

"**Maltese Data Protection Laws**" means all applicable data protection and privacy legislation in force from time to time in Malta, including (i) the Data Protection Act, Chapter 586 of the Laws of Malta; (ii) the GDPR; (iii) all national implementing laws, regulations and secondary legislation applicable in Malta which relate to the processing of Personal Data, in each case as may be amended, supplemented or replaced from time to time.

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, which, in the context of this Addendum, means: (1) Personal Data that is transferred from Client to Processor as part of the Transaction Data; and (2) Client Data which may include information provided in merchant application forms which is transferred onwards to Card Schemes. For the avoidance of doubt, to the extent that Shift4 is required to processes such Client Data for its own legal and/or regulatory requirements under the Agreement, it shall do so as a Controller. Client hereby expressly consents to Shift4's use of such data for this purpose.

"**Potential ADC**" means an occurrence that could result, directly or indirectly, in the unauthorised access to or disclosure of account data, or the unauthorised manipulation of account data controls, such as account usage and spending limits as defined by the Card Schemes.

"**Principal Contact**" means a designated person or department from Client's organisation, as provided by Client or by Provider, as applicable, by application form or other means.

"**Processor**" means Shift4, which processes Personal Data on behalf of Client.

"**Restricted Transfer**" means the international transfer of Personal Data outside the EEA, to a third country or international organisation which does not have an Adequacy Decision.

"**Services**" means the services as defined in the respective Agreement:

- Acquiring (Merchant) Agreement or Payment Facilitator Agreement: Processing of payment data for the settlement of funds to Client's bank account;
- Local Payment Methods Agreement (LPM): Provision of connectivity to payment services which are local payment methods, and which are not part of the Card Schemes as defined in the Agreement; or
- SkyTab Agreement: Provision of point of sale [POS] equipment, technical connectivity, software and gateway services for managing orders and processing payment transactions.
- Payment Gateway or Reseller Agreement: Provision of technical connectivity, and added value services, which are not regulated, as described under the Agreement.

"**Standard Contractual Clauses**" means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries, as set out in the Annex to Commission Decision 2010/87/EU, and as may be amended or replaced by the European Commission from time to time, and its application, where relevant, in accordance with the International Data Transfer Addendum to the Standard Contractual Clauses, as issued by the UK Information Commissioner's Office under S119A(1) of the Data Protection Act 2018 (the "**UK Addendum**").

"**Sub-Processor**" means a third party contracted by the Processor to process Personal Data for the purpose of carrying out a specific processing activity on behalf of the Controller in connection with the Services.

"**Supervisory Authority**" means the relevant supervisory authority with jurisdiction over the Data Protection Laws.

"Transaction Data" means any information related to a card or a payment instrument for effectuating purchases or other financial transactions. This may include card number assigned to the card by the issuing bank, cardholder/buyer name, expiration date or the card, CVV code, the name and location of the Client where the transaction occurred. Transactional Data may include Personal Data.

"**United Kingdom Data Protection Law**" means all applicable data protection on privacy legislation in force from time to time in the United Kingdom, including the Data Protection Act 2018, and all laws, regulations, and secondary legislation applicable in the United Kingdom which relate to the processing of Personal Data, in each case as may be amended, supplemented or replaced from time to time, including the UK Addendum.

2. General

2.1. Both Parties warrant that they will comply with their respective obligations under Data Protection Laws and the terms of this Addendum. As agreed between the Parties with regard to Personal Data, for the purposes of all Data Protection Laws, Client shall act as Controller and Shift4, shall act as Processor.

2.2. Subject to the provisions of the Agreement and any instruction that may be given from time to time in writing by Client, Processor is hereby appointed by Client to process Personal Data on behalf of Client for the purpose of performing and fulfilling the Services which consist of: (i) the provision of acquiring services, including, but not limited to, the processing and settlement of payment card Transactions according to regulatory and Card Scheme standards and requirements, both for point of sale and card not present ; (ii) the provision of connectivity to local payment methods and which are not part of the Card Schemes as defined in the Agreement; (iii) the provision of technical services supplementary to payment processing, including, but not limited to, the provision of gateway and smart routing services, according to regulatory and Card Scheme standards and requirements and (iv) the provision of POS equipment, software, and gateway for the management of orders, and processing of payment transactions via wi-fi and 4G connectivity.

2.3. The Parties therefore acknowledge and agree that Client retains control of Personal Data at all times. As the Controller, Client remains solely responsible for ensuring and maintaining compliance with any and all obligations which may be imposed upon Controllers of Personal Data under Data Protection Laws. This includes providing any required notices and mandatory information to Data Subjects, obtaining any required consents from Data Subjects, and for any other instructions which it may give Processor from time to time.

2.4. Where the connectivity to the Services is via Provider or other third party of the Client, Client acknowledges that the processing Transactions flow is from Merchant to Provider to Processor and is covered under this DPA, and Processor takes no responsibility for any interceptions or compromises in the Transactions data flow that is received from Provider.

3. Client's Obligations

3.1. Client warrants and represents to Processor that:

3.1.1. it shall be exclusively responsible for ensuring that it complies at all times with any and all obligations which it may have as the Controller of the relevant data under this Addendum and under the Data Protection Laws;

3.1.2. all Personal Data is obtained in accordance with the Data Protection Laws and in particular, that where it has relied on consent as a means of processing Personal Data, it has obtained valid consent of the Data Subjects as required in terms of Data Protection Laws;

3.1.3. all instructions given to Processor in terms of this Addendum and the Agreement shall at all times be in accordance with Data Protection Laws, and that the compliance, performance, or execution of any and all such instructions shall not, at any point in time, cause Processor to be in breach of any Data Protection Laws;

3.1.4. it has provided the Data Subjects with all necessary information about the processing of the Personal Data in the context of the Agreement as required by Data Protection Laws, including, without limitation, information relating to the appointment of Processors transferring to, and processing Personal Data by, third parties which may use or retain the Personal Data for compliance with legal and regulatory requirements;

3.1.5. it shall maintain all necessary policies and processes to authorise the access and processing of the relevant data in the full manner contemplated by this Addendum and the Agreement;

3.1.6. in case of a Data Breach affecting Personal Data, Client shall notify Processor immediately of becoming aware of such Breach, including the details of the Data Breach and the affected records; and

3.1.7. in case of an ADC event or a Potential ADC event is or may affect any system or environment of Client or Processor, Client shall notify Processor immediately of becoming aware of such event, including the details and the affected system or environment. Client understands and that the Card Schemes require to be informed of any Data Breach and it agrees that Processor will report any such Data Breaches to the Card Schemes. Client shall also provide Processor with the information which may be requested by Processor, in accordance with the Card Schemes requirements.

3.2. Client hereby grants its express consent to Processor communicating Personal Data to a Sub-Processor (in accordance with the requirements of this Addendum), payment scheme, Third Party Operator and relevant local and or alternative payment method schemes, an issuing bank or other participating bank, or a regulator, provided it does so in accordance with applicable law and/or as required for the performance of the Agreement.

3.3. Client acknowledges that as Controller it is Client's responsibility to provide documented instructions, which for the purpose of this DPA shall be the Agreement, upon which Processor shall rely on in order to process Personal Data for the purposes of carrying out the Services as set out in the Agreement.

3.4. Client shall pay Processor any internal costs and/or third party expenditure suffered or incurred by Processor or any of its affiliates in providing any assistance, information and cooperation pursuant to Processor's obligations as defined below.

4. Processor's Obligations

4.1. Processor shall only carry out processing of Personal Data in accordance with the written instructions provided by Client, which have been given by way of the terms of the relevant Agreement, and shall only process such Personal Data for the performance of the Services, including Restricted Transfers (unless Processor is otherwise required to process Personal Data by relevant law or any regulatory bodies to which Processor is subject, in which case Processor shall inform the Controller of that legal requirement unless prohibited by that law on grounds of public interest), and shall immediately inform Client if, in the opinion of Processor, any instruction given by Client to Processor infringes Data Protection Laws.

4.2. Processor shall comply with its obligations as Processor under the relevant Data Protection Laws.

4.3. Processor shall reasonably cooperate with Client at Client's cost, with fulfilling Client's obligations as Controller in respect of Data Subject rights under the Data Protection Laws.

4.4. Processor shall take all technical and security measures required to protect Personal Data in accordance with Article 32 of the GDPR.

4.5. Where relevant for the processing of Personal Data provided by Client and taking into account the nature of the processing and the information available to Processor, upon written request, Processor shall use all reasonable measures to assist Client in demonstrating compliance with the obligations of Client to; (i) keep Personal Data secure at all times; (ii) implement and maintain appropriate technical and organisational measures to protect against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of the Personal Data and against accidental or unlawful loss, destruction alteration, disclosure or damage to the Personal Data, including but not limited to, the security measures as set out in the Agreement.

4.6. In case of a Data Breach, Processor shall, as soon as reasonably possible after becoming aware, inform Client of any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access or any other form of unauthorised processing, or of any disruptions endangering the security of Data Subject's Personal Data, or Personal Data transmitted, stored or otherwise processed. Processor accepts and acknowledges that Client may take steps and measures to remedy a breach by Processor under Data Protection Laws, including but not limited to any communications with a Supervisory Authority, unless otherwise required by law.

4.7. On expiry or termination of the Agreement, Processor shall cease to use Personal Data and shall arrange for its safe return or destruction as shall be required by Client unless Applicable Law requires storage of any Personal Data, or an exemption under GDPR applies.

4.8. Upon written request, Processor shall make available to Client all information necessary to demonstrate compliance with the obligations under Data Protection Laws and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client in accordance with Clause 5 below.

5. Audit Rights

5.1. Upon Client's reasonable prior written request, and no more than once a year, unless such request is in relation to a breach by Processor, Processor agrees to provide Client with documentation or records (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) to demonstrate Processor's compliance with its data protection and security obligations under the terms of this Addendum. Processor shall provide such information within sixty (60) days of receipt of such request and notify Client of the person within Processor's organisation who will act as point of contact for the provision of the information required by Client.

5.2. Where, in the reasonable opinion of Client, such documentation is not sufficient in order to meet the obligations of Article 28 of the GDPR, Client will be entitled, upon providing thirty (30) days prior written notice to Processor and upon reasonable grounds, to conduct an on-site audit of Processor's premises used in connection with the Service under the relevant Agreement, solely to confirm compliance with its data protection and security obligations under this Addendum. Any such audit will be limited in time and shall last no longer than three (3) business days, during business hours.

5.3. Any type of audit carried out by Client will be conducted in a manner that does not disrupt, delay, or interfere with Processor's performance of its business. Client shall ensure that the individuals carrying out the audit are under the same confidentiality obligations as set out in the Agreement. Depending on the effort estimated by Processor, costs incurred with respect to an audit or request for documentation or records, will be borne by Client.

5.4. Any audit right granted to Processor under the Agreement shall remain in full force and effect. In the event that there is no audit right in favour of Processor or the audit right contained in the Agreement in favour of Processor is not sufficient to enable it to verify and monitor Client's compliance with its data protection and security obligations under the terms of this Addendum, then, Processor shall be entitled to carry out an audit of Client on reciprocal terms as those set out in this clause.

6. Use of Sub-Processors

6.1. Client hereby authorises and grants Processor general written authorisation to appoint Sub-Processors (and further permits each Sub-Processor appointed in accordance with this provision, to appoint Sub-Processors) in accordance with this provision and any restrictions contained in the Agreement.

6.2. Processor shall notify Client of any changes concerning the addition or replacement of Sub-Processors and allow Client thirty (30) days to object such changes. Should Client object Processor's changes, it shall allow Processor to address Client's concerns and mitigate them. Where Client's objection persists, it may terminate its Agreement with Processor.

6.3. Processor shall remain liable to Client in the event that the Sub-Processor fails to fulfil its data protection obligations and for all other actions and omissions of the Sub-Processor, as required under GDPR.

6.4. Processor shall bind its Sub-Processors in terms of this clause by means of a written contract that contains processing clauses and obligations substantially the same as those set out in this Addendum.

6.5. A list of Processor's current Sub-Processors can be found in Annex III. By entering into the Agreement, Client acknowledges and accepts the use of these Sub-Processors.

6.6. For Services received under the Technical Services Agreement or Reseller Agreement, Client acknowledges that it is aware that the list of Sub-Processors may change in accordance with the Services chosen.

7. Processor's Employees

Processor shall ensure that its employees and other personnel who are given access to Personal Data are adequately and responsibly informed of the confidential nature of the Personal Data and have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality.

8. International Transfers

8.1. In order to provide the Services, Processor transfers Personal Data outside the EEA.

8.2. Client hereby agrees that Processor may transfer Personal Data outside the EEA on the basis of an Adequacy Decision, or subject to appropriate safeguards, as allowed under the GDPR.

8.3. Client hereby grants a general mandate for Processor (acting as a data exporter) to enter into and sign Standard Contractual Clauses with any Sub-Processor (acting as a data importer) located in a jurisdiction without an Adequacy Decision. Client understands that without such Restricted Transfer, Processor is unable to provide the Services.

8.4. Where Personal Data originating in the EEA is transferred by Processor to outside the EEA to a territory that has not been given an Adequacy Decision, the Client and Processor agree that the transfer of such Transaction Data between the Processor and any Sub-Processor shall be subject to **Module Three** (Transfer processor to processor) of the Standard Contractual Clauses, and where the transfer is subject to United Kingdom Data Protection Laws, the Standard Contractual Clauses shall be read in accordance with, and deemed amended by the provisions of **Part 2** (Mandatory Clauses) of the UK Addendum.

8.5. The relevant provisions contained in the Standard Contractual Clauses and the UK Addendum are incorporated by reference and are an integral part of this Addendum.

8.6. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Annexes I, II, and III of this Addendum.

I. Annex I - Description of onward transfer under standard contractual clauses between Processor and Sub-Processor

II. Annex II - Technical and organisational measures including technical and organisational measures to ensure the security of the data

III. Annex III – List of Sub-Processors

8.7. For the purposes of Table 4 of Part One (Tables) of the UK Addendum, the Parties shall select the “neither party” option.

9. Security

9.1. For the avoidance of doubt, both Parties acknowledge that any provisions in relation to PCI-DSS used in connection with the Processor Services under the Agreement shall remain unchanged and in full force and effect.

9.2. Parties warrant and agree that each shall carry out and implement any security measures (technical and organisational) which may be necessary or otherwise mandated under Data Protection Laws (specifically with respect to Article 32 of the GDPR) to safeguard the privacy and security of the Personal Data, and that these measures shall remain in place for the duration of the Agreement. This will include ensuring that there are sufficient technical and organisational measures to ensure data protection by default and by design.

10. Liability & Indemnity

Subject to the liability clauses in the Agreement, the Parties further agree that they will be held liable for violations of Data Protection Laws towards Data Subjects as follows:

10.1. Client shall be liable for the damage caused by the processing of Personal Data which infringes Data Protection Laws or this Addendum where it has not complied with obligations of Data Protection Laws specifically directed to Controllers.

10.2. Client shall indemnify, defend, and hold Processor harmless from and against any and all claims, actions, suits, demands, assessments, or judgments asserted, and any and all losses, liabilities, damages, costs, and expenses (including, without limitation, attorneys fees, accounting fees, and investigation costs to the extent permitted by law) alleged or incurred arising out of or relating to any operations, acts, or omissions of Client or any of its employees, agents, and invitees in the exercise of Client's rights or the performance or observance of the Client's obligations under this agreement. Prompt notice must be given of any claim, and the Client providing the indemnification will have control of any defence or settlement.

10.3. Processor shall be liable for the damage caused by the processing of Personal Data which infringes Data Protection Laws or this Addendum only where it has not complied with obligations of Data Protection Laws specifically directed to Processors, or where it has acted in breach of its obligations under this Addendum. In that context, Processor as Processor will be exempt from liability if it can prove that it is not in any way responsible for the event giving rise to the damage. In accordance with Article 82 of the GDPR

10.4. Processor's liability shall be limited in accordance with the limitation on liability clause in the relevant Agreement. To the extent that Processor processes Personal Data under more than one Agreement for Client, Client may only make one claim in relation to such Personal Data, and Client shall not be entitled to additional indemnification, and Processor shall not be liable for any additional damages.

11. Applicable Law and Jurisdiction

This Addendum is subject to the conditions stipulated in the Agreement.

12. Notice

12.1. Any notice or other communication relating directly to this Addendum are to be given in writing to DPO@Shift4.com. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

12.2. Processor shall provide notices relating to this Addendum, including breach notifications and other privacy related matters, to the Principal Contact. To the extent Client is a Merchant that receives the Services via Provider, Processor shall provide notices relating to this Addendum to such Provider, and it is such Provider's responsibility to notify Merchant accordingly. It is Client's responsibility to update Processor in case of any changes in the Principal Contact.

13. SKYTAB and other CARD PRESENT services offered by Shift4 – ADDITIONAL TERMS:

13.1. If Client is receiving SkyTab and Card Present services from Shift4, via a third party dealer, partner, referrer, integration ("Third Party Operator") , Client may receive assistance, support and other ancillary services from Third Party Operator. Client instructs Shift4 to enable access to Client's data and Personal Data to Third Party Operator to provide said assistance.

13.2. Client further confirms that it has given its express permission to Third Party Operator to: (i) process Personal Data as may be required, including access to Personal Data held on Processor platforms, and (ii) receive credentials to access Shift4's platforms, information and Personal Data.

13.3. Client will hold Processor harmless, and shall indemnify Processor in full for damage caused by Third Party Operator's uses, breaches or misuses that may occur with respect to Third Party Operator accessing and using Client Personal Data, including any claims that may arise from Data Subjects or from Shift4.

13.4. Furthermore, Client waives its right to bring a claim against Processor for granting such access, or for any outcome caused by granting such access.

ANNEX I –

DESCRIPTION OF ONWARD TRANSFER UNDER STANDARD CONTRACTUAL CLAUSES BETWEEN PROCESSOR AND SUB-PROCESSOR

Data exporter

The data exporter is:

Transferring Personal Data for the provision of the Services as detailed in the relevant Agreement, including:

For Acquiring, LPM, or Payment Facilitator Agreements: the processing of Personal Data for the settlement of funds to Controller as detailed in the relevant Agreement.

For Payment Gateway or Reseller Agreements: the processing of Personal Data for the provision of technical services supplementary to payment processing, in accordance with the Services selected under the Agreement. Further, as may be relevant, the provision of point of sale equipment (payment pinpad)

For Skytab Services: Provision of point of sale [POS] equipment, connectivity and software for managing and processing payment transactions Data importer

The data importer is:

Processing Personal Data to enable and facilitate the provision of the Services detailed in the Agreement, and as detailed in the Sub-Processors list.

Data subjects

The Personal Data transferred concerns the following categories of data subjects:
Cardholders or shoppers or buyers of Controller;

Categories of data

The Personal Data transferred concerns the following categories of data:

Encrypted credit card number, name, email, address, IP address and any other information transferred by Controller.

Special categories of data (if appropriate)

The Personal Data transferred does not fall under a special category of data

Processing operations

The Personal Data transferred will be subject to the following basic processing activities:
Processing, storing, analysing, visualising, and monitoring data.

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

- Data encryption as required by applicable PCI standards.
- Compliance programme.
- Data privacy by default and design – Consistent data classification and definition of related security controls are completed for all procurement and development processes.
- Vendor risk management - Additional supplier audits and security scans are included into the life cycle of high risk vendors.
- Management review - CISO and CIO approval is required for any new supplier with remote connection to production environment.
- Privacy Legal controls – DPO approval and Privacy Team review is required for any new supplier with access to PII data. These suppliers sign a DPA and their employees that have access to PII data sign additional documentation: WISP, AUP, and an NDA. Shift4 employees also sign these documents.
- Privacy and Security lectures, Tutorial videos and E-learning – –Based on a yearly workplan dedicated training and GDPR courses for employee onboarding tailored for role, with additional annual training per department.
- Phishing campaigns – each quarter with additional training and explanation video for “easy clickers.”
- Digital footprint –GDPR compliance for Sales & Marketing tools like Privacy policy, Cookie's policy, GDPR consents management system with automated workflows.
- Centralised management – Fully automated based with additional security assessment.

ANNEX III – SUB-PROCESSORS

List of Sub-Processors can be found here:

https://www.shift4.com/s4i-sub-processors

Version History:

Unified Version:
Version 2 - Effective 1st December 2024
Version 1 – 1st February 2024 - 1st December 2024

Previous DPAs replaced by Unified Version

Acquiring/ Local Payment Methods DPA - https://www.shift4.com/s4i-gdpr

Payment Facilitator DPA - https://www.shift4.com/s4i-pf-gdpr

Reseller/Technical Services DPA - https://www.shift4.com/s4i-ssm-gdpr