

1 Organizational Setup at LP

1.1 Please name the vendor providing the services to LP. Enter the exact legal entity.

The decisive factor here is the legal entity with which the contract is ultimately concluded.

Response

Other

1.2 Please indicate for which companies of LP the service is/will be provided.

Response

Not Answered

1.3 Please specify the responsible business.

If not shown here, please contact PAYBACK Operational Excellence Team.

Response

Not Answered

1.4 Please state the e-mail address of the cost center and/or budget manager (business owner).

Response

Not Answered

1.5 Please indicate in which phase of the contract we are currently in.

Response

Active & Existing Contract

New Contract (signed)

New Contract Under Negotiation (not signed)

1.6 Please indicate the contract term for which the service contract is to be concluded.

Response

Not Answered

1.7 Please state the e-mail address of the LP Procurement point of contact.

Response

Not Answered

1.8 Please indicate name and surname of the LP contact person responsible for the vendor.

Note:

The Third Party Relationship Manager (TRM) will be responsible for coordinating the vendor onboarding process including pre- & post-contract audit requirements (American Express Management Policy 10).

Response

Not Answered

1.9 Please state the e-mail address of the LP employee directly responsible for the vendor in question. If available, please directly indicate the American Express e-mail address.

Note:

The Third Party Relationship Manager (TRM) will be responsible for coordinating the vendor onboarding process including pre- & post-contract audit requirements (American Express Management Policy 10).

Response

Not Answered

1.10 Please indicate name and surname of the supervisor of the LP TRM (TRM Lead).

The TRM Lead will be responsible for quality assurance and makes sure that stated attributes of the vendor relationship are stated correctly by the LP TRM (LP vendor manager).

Response

Not Answered

- 1.11 **Please provide the e-mail address of the vendor manager's supervisor. If available, please directly indicate the American Express e-mail address.**

Note:

The TRM Lead will be responsible for quality assurance and makes sure that stated attributes of the service/vendor relationship are stated correctly by the TRM.

Response

Not Answered

- 1.12 **Please indicate name and surname of the person who will monitor the performance of the vendor (Performance Manager).**

Note:

the Performance Manager is responsible for the so-called "Ongoing Oversight" as part of the AXP-TLM process (optional requirement). This role requires an AXP-ADS account (AXP e-mail address). The transmission of suitable metrics/performance data usually takes place quarterly. If you already have an AXP e-mail address to state here, please enter it. If this is not the case, the LP/PAYBACK e-mail address is sufficient as placeholder.

Response

Not Answered

- 1.13 **Please indicate the e-mail address of the the person who will monitor the performance of the vendor (Performance Manager). If available, please directly indicate the American Express e-mail address.**

Note:

the Performance Manager is responsible for the so-called "Ongoing Oversight" as part of the AXP-TLM process (optional requirement). This role requires an AXP-ADS account (AXP e-mail address). The transmission of suitable metrics/performance data usually takes place quarterly. If you already have an AXP e-mail address to state here, please enter it. If this is not the case, the LP/PAYBACK e-mail address is sufficient as placeholder.

Response

Not Answered

2 Information related to the Vendor

- 2.1 **Please state name and surname of the relevant contact person at the vendor.**

Response

Not Answered

- 2.2 **Please enter the e-mail address of the relevant contact person at the vendor.**

Response

Not Answered

- 2.3 **Please enter the telephone number of the relevant contact person at the vendor.**

Note:

Alternatively, the telephone number of the company headquarters can also be used.

Response

Not Answered

- 2.4 **Please enter the street and house number of the vendor's local headquarters.**

Response

Not Answered

- 2.5 **Please enter the city of the vendor's local headquarters.**

Response

Not Answered

- 2.6 **Please enter the postal code of the vendor's local headquarters.**

Response

Not Answered

2.7 Please indicate the country in which the vendor's local headquarters is located.

Response

Not Answered

2.8 Please indicate the size of the vendor by stating its approximate number of employees.

Note:

Please provide the information for the service provider/vendor's legal entity which will engage into the contractual relationship with LP.

Please be as exact as possible as this information has direct impact on the information security risk rating. The information can either be retrieved through the suppliers website or through the direct point of contact.

Response

< 10

Employees

11 to 100

Employees

101 - 500

Employees

501 -1000

Employees

> 1000

Employees

2.9 Is the vendor publicly traded on one of the recognized stock exchanges?

Note:

If the **parent company** controlling the vendor is publicly traded on one of the recognized stock exchanges, please answer "Yes" as well.

The information can either be retrieved through the suppliers website or through the direct point of contact.

Response

Yes

No

3 Information related to the Service

3.1 Have legal aspects of the terms and conditions been reviewed by the relevant department(s) (Data Privacy & GCO)?

If not, please provide a reasoning in the comment box.

Response

Yes

No

3.2 Please indicate the total spent (in USD) over the lifetime of the contract.

Note:

If not known exactly, an approximation is sufficient.

Please indicate the cost in US-Dollar and only use digits from 0-9.

Example: 100000.

Response

Not Answered

3.3 Please describe the service delivered by the vendor in as much detail as possible.

Note:

Please describe the delivered service in chronological order and give as much detail as possible in continuous sentences.

An enumeration using bullet points is not regarded sufficient by AXP TLM. The time needed for onboarding a new vendor/service is drastically reduced by delivering accurate information from the start.

Response

Not Answered

3.4 **Please indicate where the service is being delivered from.**

Note:

Please enter the international country codes in the text field.

Example: Germany = GER

If several countries are involved for the service delivery, please note this as follows:

Example Germany & Austria: GER; AUT

Response

Not Answered

3.5 **Please indicate all target countries in which the service for the Loyalty Partner Group is being provided.**

Note:

Please enter the international country codes in the text field.

Example: Germany = GER

If several countries are involved for the service delivery, please note this as follows:

Example Germany & Austria: GER; AUT

Response

Not Answered

3.6 **Please indicate whether personal data is shared/collected within the scope of the service.**

Note:

Please indicate in the comment field which data elements are involved. Examples of personal data are among others:

Address - Business / Home

E-mail address (business or personal)

Telephone number - business / private / mobile / mobile

Fax number (business or personal)

Last name plus first name or first initial

PAYBACK customer number / PAYBACK reference ID

IP-Address

Mother's maiden name

Identity card/passport number

driver's license number

Security questions and/or answers

Social security number - complete

Note 2:

If you have any questions about the concrete interpretation of data not mentioned here, please contact your LP GCO (Legal) Team.

Response

Not Answered

3.7 **Please indicate where the collected/shared/processed data will be stored.**

Note:

To answer this question, please contact the person responsible for IT at the service provider.

If needed, LP Information Security will assist you with that question.

Response

Not Answered

3.8 **Please name the involved cloud service provider the vendor and/or the service is using.**

Note:

If required, LP Information Security will assist you with that question. If not listed here - please specify using "Other".

Response

Not Answered

3.9 Please indicate at how many physical locations data involved in the procured service will be stored.

Note:

The address(es) have to be provided as part of the following question.

Response

- ☐ 1
 ☐ 2
 ☐ 3
 ☐ 4
 ☐ 5
 ☐ >5

3.10 Please enter the address(es) where shared data will be physically stored. If there are multiple hosting locations, please name all.

Note 1:

Please enter the address(es) as follows in the text window:

1. Sample company 1, Sample street 12, Postcode; City, Federal state, Country;
2. Sample company 2, Sample street 12, Postcode; City, Federal state, Country;
3. Sample company 3, Sample street 12, Postcode; City, Federal state, Country;
4. ...

Note 2:

If the data should take place directly at the location of the service provider (self-owned hosting infrastructure), please enter this address.

If cloud services are used, it is sufficient to indicate the respective service provider. Example: AWS (Amazon Web Services).

Response

Not Answered

3.11 Please indicate how for the service relevant information will be exchanged.

Note:

Please see below description for guidance. If unsure, LP IT/ Information Security will assist you with that question.

HTTP = Do you access/share/collect/process the data from a website that begins with "http://"? "Hypertext Transfer Protocol." HTTP is the protocol used to transfer data over the web. It is part of the Internet protocol suite and defines commands and services used for transmitting webpage data.

HTTPS = Do you access/share/collect/process the data from a website that begins with "https://"? Hyper Text Transfer Protocol Secure is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.

SFTP = Do you access/share/collect/process the data from a file transfer application? SSH File Transfer Protocol is a network protocol that provides file access, file transfer, and file management over any reliable data stream.

API = Do you access/share/collect/process the data through an application that uses API calls? API is short for Application Programming Interface. It acts as a medium between two communicating entities or applications.

Unstructured = Unstructured data files often include text and multimedia content. This would include but not be limited to; e-mail messages, word processing documents, videos, photos, audio files, web pages, social media pages, or presentations.

MPLS Direct Connections = MPLS is a networking protocol that uses a pre-determined path to the destination router. As MPLS has a highly deterministic routing. In effect it creates a VPN-type service that makes it logically impossible for data from one network to be mixed in or routed over to another network. However, MPLS does not include encryption services so the traffic is visible to service providers along the route.

Response

- ☐ HTTP
 ☐ HTTPS
 ☐ SFTP
 ☐ API
 ☐ Unstructured
 ☐ MPLS Direct Connections

3.12 **What is the expected/estimated annual volume of data records being shared/accessed/collected/created/stored and/or destroyed by the third party?**

Note:

This information will be used to further evaluate information security risk (AXP TLMP). The number should only reflect unique data records. If for example the information about a customer is shared twice during a year it would still be considered as 1 unique data record.

Response

0 to 100 Records	101 to 10,000 Records	10,001 to 50,000 Records
50,001 to = 1MM Records	1MM+ to 5MM Records	5MM+ to 10MM Records
10MM + Records		

3.13 **Which most closely represents the frequency at which data is being exchanged?**

Note:

This information will be used to further evaluate information security risk (AXP TLMP).

Response

Daily	Weekly	Monthly
Quarterly	Annual	One-time sharing/transfer of data

3.14 **Does the service provided by the vendor include a financial transaction system or the creation of monetary instruments (plastic, traveler's checks, etc.)?**

Note:

This question aims at services which are subject to banking regulation.

Response

Yes	No
-----	----

3.15 Please indicate how the data shared with the service provider is to be classified.

Note:

Always choose the classification which describing the the most sensitive data element of the service. If PII are processed as part of the service, the classification can never be "LP/AXP Public" or "LP/AXP Internal". The following are indications for the respective data class. The comment function can be used in case of ambiguities.
If unsure, please contact LP Information Security.

Note 2:

The PB card/customer number in its plain form (used to collect points) is considered "LP/AXP Business Restricted" information, as it is part of the customer login credentials.
All variations of the card/customer number (i.e. External Member ID, SCRID, Reference ID) can be considered as "LP/AXP Internal", as the externally derivable value is limited only.

LP/AXP Public:

Information/data that is already publicly accessible. They can be shared with the public. This data does not require special security controls. The loss of data classified as LP/AXP Public is uncritical and has no legal consequences.

LP/AXP Internal:

Information/data used to support normal business operations.
This information/data is defined as insensitive but requires appropriate controls.

LP/AXP Business Restricted:

Information/data is sensitive and/or gives the company a competitive advantage. A loss could affect the Company's competitiveness, the privacy of customers or employees, and the Company's legal or financial position. Access to this information is usually limited to certain groups.

LP/AXP Secret:

Information/data is very sensitive and/or gives the company a competitive advantage. A loss could seriously jeopardize the company's competitiveness, the privacy of customers or employees, and the company's legal or financial situation. Access to this information is oalways limited to specific individuals or small groups.

Response

Not Answered

3.16 **Will the service only involve the processing/sharing of "LP/AXP Public" and/or "LP/AXP Internal" data?**

Note:

- 1) In case of customer related personally identifiable information being (PII) involved, this question must be answered with "no".
- 2) In case of employee related personally identifiable information (PII) being involved, this question must be answered with "no".
- 3) If **employee** related personally identifiable information (PII) is only being shared for contact/informative purposes and other than that only LP Public/Internal data is shared this question can be answered with "yes".

LP/AXP Public:

Information/data that is already publicly accessible. They can be shared with the public. This data does not require special security controls. The loss of data classified as LP/AXP Public is uncritical and has no legal consequences.

LP/AXP Internal:

Information/data used to support normal business operations.

This information/data is defined as insensitive but requires appropriate controls.

Note 2:

If in doubt - please contact either LP GCO / LP Data Privacy / PB Operational Excellence / PB Information Security for clarification. This information will be relevant for the AXP information security evaluation within the TLM Process.

Response

☐ Yes ☐ No

3.17 **Is the annual volume of exchanged records below 101 AND can the exchanged/processed/shared data be classified as "LP/AXP Public", "LP/AXP Internal" or "LP/AXP Business Restricted"?**

Note:

This information will be relevant for the AXP information security evaluation within the TLM Process.

Response

☐ Yes ☐ No

3.18 **Does the service provided belong to one of the following service types?**

Service Types:

- Office Supplies
- External legal council & other necessary experts managed by LP GCO
- Travel & Entertainment expenditure
- Government Authorities and Utilities that would not normally be willing to negotiate pricing or contractual terms

Please also answer "yes" if one of the following is true:

- Third party is considered to be LP/AXP customer/partner (i.e. Classic, OOP, Affiliate Partners)
- Third party is considered to be a Joint Venture and Controlled Entity (by LP/AXP)

Response

☐ Yes ☐ No

3.19 Are 4th parties (subcontractors) involved in the provision of the service?

Note:

4th parties (subcontractors) are those players who do NOT have a direct contractual relationship with the LP Group, but who take over parts of the services via a separate service provider contractual relationship (subcontractor).

If a 3rd party (vendor/service provider) has suppliers that they use to support their own business, such as payroll, HR Support, Travel Management, etc., then those would not be considered 4th parties to LP/AXP. Only their suppliers that support the work the 3rd party does for LP/AXP would be considered 4th party to LP/AXP.

Response

☐ Yes ☐ No

4 Subcontractor Information - Address Info & Service

4.1 How many 4th parties (subcontractors) will be used by the vendor/service provider to fulfill their obligations under this service contract with LP/AXP?

Response

☐ 1 ☐ 2 ☐ 3
☐ 4 ☐ 5 ☐ > 5

4.2 What percentage of the original service will be completed by the sub-contractor (4th party)?

Purpose:

This purpose of this question is to understand how much of the service is being performed by the Third-Party and how much of the service is being performed by 4th parties.

A higher percentage being performed by 4th parties could result in increased risk exposure to certain risks. It is important to take this into consideration in the assessment of the overall risk.

Note:

As a rule of thumb, if a service being provided by the 3rd party (vendor/service provider) to LP/AXP is entirely accessed via a hosted site, then you can answer "25% - 74%".

If only a portion of the service is accessed via a hosted site, then this may be a lower percentage.

Response

☐ 1-24% ☐ 25-74% ☐ 75-100%

4.3 Will any of the 4th parties have access to Non-Public LP/AXP data while fulfilling their obligations under this service contract with LP/AXP?

Purpose:

When a Third-Party and one of its 4th parties have access to LP/AXP data, this can significantly increase the risk of the 3rd party service relationship. LP/AXP has an obligation to understand when 4th parties have access to Non-Public LP/AXP data, so we can work together with our 3rd party to make sure the data is protected appropriately to protect the company and its customers and colleagues. Non-Public LP/AXP data is data that is classified as anything other than LP/AXP Public using the standard LP/AXP Data Classifications. We may be asked by regulators for a list of companies that have access to our data.

Response

☐ Yes ☐ No

- 4.4 **Please list the 4th parties that have access to Non-Public LP/AXP data with their current addresses. Please use the following format for the text window:**

1. Sample company 1, Sample street 12, Postcode; City, Federal state, Country;
2. Sample company 2, Sample street 12, Postcode; City, Federal state, Country;
3. Sample company 3, Sample street 12, Postcode; City, Federal state, Country;
4. ...

Response

Not
Applicable

- 4.5 **Are any of the 4th parties critical to the continuity of the services being provided under this service contract with LP/AXP?**

Purpose:

When one or more 4th parties are critical to the ability of a 3rd party (vendor/service provider) to fulfill their obligations to LP/AXP, it can increase the risk of the 3rd party relationship. A 4th party would be considered "critical" if it is necessary for the 3rd party to deliver the service. For example, LP/AXP retains a Marketing Agency to build and manage a site that is hosted by a 4th party. The site would not function if it were not hosted, so this 4th party is considered critical.

Response

Yes No

- 4.6 **Please list the 4th parties that are critical to the continuity of the services being provided with their current addresses. Please use the following format for the text window:**

1. Sample company 1, Sample street 12, Postcode; City, Federal state, Country;
2. Sample company 2, Sample street 12, Postcode; City, Federal state, Country;
3. Sample company 3, Sample street 12, Postcode; City, Federal state, Country;
4. ...

Response

Not
Applicable

- 4.7 **Do any of the 4th party relationships with the 3rd party have an element of sales incentive compensation to drive the performance of the 4th party?**

Purpose:

When a 3rd party uses a 4th party to help sell goods and/or services on behalf of LP/AXP, this can significantly increase the risk of the 3rd party relationship. LP/AXP has an obligation to understand when 3rd parties are using a 4th party to help sell goods and/or services on behalf of LP/AXP so we can work together with our 3rd party to make sure they are fulfilling their obligations to LP/AXP and that they are complying with Consumer Protection laws.

Response

Yes No

- 4.8 Will any of the 4th parties have direct interaction with LP/AXP customers while fulfilling their obligations under this service contract with LP/AXP?

Response

☐ Yes ☐ No

- 4.9 Select all service activity(ies) that are or will be conducted by the 4th parties to fulfill their obligations to this service contract with LP/AXP.

Response

a. Sales Related Activities	b. Distribution Related Activities	c. Customer Service Related Activities
d. Account Fulfillment Related Activities	e. Collections and Credit Related Activities	f. Marketing and Advertising Related Activities
g. Reward / Benefit Fulfillment Activities	h. Data Center Provider	i. Payment Processing Related Activities
j. Merchant Acquisition Related Activities	k. Data Capture / Data Entry	l. Hardware Supplier
m. Software Related Services	n. Public Relations Related Services	o. Transportation and Data Storage Services
p. Human Resource Related Activities	q. Market Research / Data Brokerage Services	r. Consulting
s. Staffing Related Services	t. Intermediary	

5 Service Risk Assessment

- 5.1 SRA 1: Is any data that could identify an individual or could be used in combination with other information to identify an individual (also known as Personal Data or personally identifiable information (PII)), being processed?

Note:

This question must also be answered with "Yes" in the case of pseudonymised/aggregated personal/personal data. In the case of irretrievably anonymous data, the question can be answered with "No". In AXP risk context, the PAYBACK customer number and the PAYBACK Reference ID are NOT regarded as personal characteristics. Processing of Personal Data/PII refers to any action taken in relation to Personal Data/PII and includes collecting, storing, altering, accessing, using, transferring, receiving, sharing or destroying Personal Data/PII.

Examples include:

Address - Business / Home
 E-mail address (business or personal)
 Telephone number - business / private / mobile / mobile
 Fax number (business or personal)
 Last name plus first name or first initial
 IP-Address
 Mother's maiden name
 Identity card/passport number
 Driver's license number
 Security questions and/or answers
 Social security number - complete

If there is any doubt about the classification of the data, please contact the responsible data protection officer (InfoSec) or GCO.

Response

☐ Yes ☐ No

- 5.2 SRA 2: Will the proposed Service/ activity require the third party to support a Critical Business Function (CBF) i.e. BIA Tier 1-4?

Critical business functions typically include directly attributable revenue, the exchange of confidential/sensitive information, or the potential for negative customer or partner perceptions in the event of failure. If unsure, please contact your BC-Coordinator (AXP role) for your respective line of business.

Response

☐ Yes ☐ No

5.3 **SRA 3a: Does the service provided by the vendor involve any of the following “Critical or High Compliance Risk” activities?**

- Sales
- Servicing (Specifically Customer Servicing)
- Marketing & Advertising
- Collections & Credit
- Account Fulfillment
- Insurance Tele-Marketing Agency

Response

☐ Yes ☐ No

5.4 **SRA 3b: Does the service provided by the vendor include any of the following activities?**

- Reward Processing and Fulfillment
- GMS Acquiring Service Provider – International Only
- HR Services (Car Leases, Employee-Benefit Mandatory (mandated by law)* Payroll, Pensions –Mandatory (mandated by law), and Recruitment Process Outsourcers (RPOs)
- Market Research
- Sweepstakes
- Non-Merchant Lead Generation/Provider
- POP Provider-Distribution Only and/or Field Marketing Third-Party
- Marketing, Adv-Banners/Billboards
- Marketing & Advertising: Media Buy & Placement
- Sponsorship Experiential
- No Additional Charge (NAC) Insurance Provider

Response

☐ Yes ☐ No

5.5 **SRA 6: Will the service involve collaboration or confidential information sharing with a direct competitor of LP/AXP or will the service directly limit the ability of LP/AXP competitors to compete?**

Response

☐ Yes ☐ No

5.6 **SRA 7: Will the service initiate financial transactions on behalf of LP/AXP or affect LP/AXP financial statements?**

Response

☐ Yes ☐ No

5.7 **SRA 8: Will the Service include access to, process, collect, share, create, store and/or destroy any LP/AXP data (Company, Employee, and/or Customer Information) and/or have access to LP/AXP Systems?**

Note:

There are two aspects to this question which are equally important - please consider both when answering:

1) Type of exchanged data (the type of exchanged data has already been defined in question 3.14)
 LP/AXP Public - Only already publicly accessible information (SRA 8 = No)
 LP/AXP Internal - Data concerning operational business processes (SRA 8 = No)
 LP/AXP Restricted - Sensitive data: Customer data, partner data, restricted user group (SRA 8 = Yes)
 LP/AXP Secret - Highly sensitive data: Passwords, individual users (SRA 8 = Yes)

2) Access to LP/AXP systems - Question to be answered "Yes" if any of the following is true:
 Direct system interfacing (i.e. through SDK/API implementation/connection)
 Direct access to our systems (i.e. through external user accounts)

Please contact LP IT/Information Security if you need assistance in answering this question.

Response

☐ Yes ☐ No

5.8 **SRA 9: Does the third-party have ANY government ownership or government control?**

Response

☐ Yes ☐ No

5.9 **SRA 10: Will the service or activity provided by the third party involve or potentially involve interaction with government entities in order to fulfill its contractual obligations (i.e. is the third party an intermediary)?**

Response

☐ Yes ☐ No

5.10 **Is the service provider incentivized with a payment, award or any other transfer of value for achieving defined targets based on the service that is outsourced to them?**

LP/AXP uses various programs to promote its products and services and to provide incentives for customers and other external business partners ("external parties") to make use of LP/AXP products and services. Programs that provide benefits in exchange for meeting certain sales, volume, timing, or other defined targets; raffles and sweepstakes; and surveys in which items of value are provided to survey participants in exchange for their participation.

Response

☐ Yes ☐ No

6 Additional Information

6.1 **Does the service provider have additional documents/certifications regarding its data security?**

Please add the relevant documents.

Response

ISO 27001 Certification	BS 10012 Certification	SOC 2 Report
SIG Questionnaire	CSA CAIQ	CSA STAR
Approved GDPR Code of Conduct	Approved GDPR Certification Mechanism	Privacy/Security Whitepaper
Privacy Notice	Not Applicable	Other

6.2 **Optional: Please add additional information here.**

Response

Not Answered