Policy Name	:	Loyalty Partner Confidentiality Operating Principles
Approval Requirement	:	AXP General Counsel Officer
Effective Date	:	July 1st 2016
Prepared by	:	Wiebke Strachwitz
Policy Owner/Custodian	:	Network Information Control Officer
Next Scheduled Review	:	May 2018

Changes to Previous Policy:

Change of the Network Information Control Officer

- Extension of scope to Payback new markets

Table of Content

1 OVERVIEW AND PURPOSE

In 2011 American Express (***AXP***) acquired control of Loyalty Partner Group, a business which – through subsidiaries - operates multi-partner loyalty programs in Germany, Poland, India as well as providing customer relationship management, business process outsourcing and consulting services associated with the loyalty- and other marketing programs (***LP***).

As a result of its business activities, LP has access to a range of information regarding partners who participate in its loyalty programs, customers who earn points in those programs and other clients who engage LP for consulting and outsourcing services. This includes commercially sensitive information, information which is deemed confidential under a contract (even if not patently sensitive), and personal data (***Confidential Information***). Examples of Confidential Information of partners are set out at the end of this policy.

LP contracts with its partners and clients generally contain provisions requiring it to protect third party confidential information and restrict the disclosure and use of such information. In addition, both LP and AXP must comply with applicable regulation, including competition rules, which prohibit the exchange of commercially sensitive information between competitors, and data protection rules, which protect unauthorized dissemination and use of personal data.

In order to ensure that LP and AXP meet their contractual and legal obligations, these LP Confidentiality Operating Principles (***LPCOP***) set out the principles under which Confidential Information may be disclosed to employees of AXP outside of the LP business. Other commercial or reputational considerations may also apply; however, these are not addressed by the LPCOP.

Although not the focus of the LPCOP, please keep in mind that:

- to the extent LP receives confidential information of AXP, such information must not be shared with third parties by any LP or AXP employee except in accordance with applicable AXP policies; and
- similar issues and restrictions apply in relation to any potential disclosure Confidential Information to third parties outside AXP (e.g. other partners, prospective partners, etc.).

2 ROLES & RESPONSIBILITIES

All LP employees

Every employee working as part of the LP business is responsible for safeguarding information received in the ordinary course of his or her job responsibilities. This includes contractors, AXP employees and any third party vendor employees who come from outside the LP business but who are assigned to work on LP business. This responsibility includes taking appropriate steps to protect Confidential Information, contacting the Network Information Control Officer in the General Counsel's Organization (***GCO***) upon becoming aware of policy violation, and ensuring that any service provider that handles Confidential Information on behalf of LP is aware of and has agreed to comply with the LPCOP.

Network Information Control Officer

The Network Information Control Officer for the LPCOP is the Head of GCO at LP in Munich (currently Bernd Wagner) or his delegate (as appointed generally or on a case-by-case basis).

For support or clarification related to any approval request, exception, conflict or interpretation resolutions, please contact lpcop@loyaltypartner.com.

3 POLICY REQUIREMENTS

The LPCOP defines three basic principles to govern how LP uses and safeguards Confidential Information of its partners, customers and clients.

The LPCOP principles are:

1. LP must comply with all applicable laws and regulations on the sharing and use of information it holds.

2. LP must comply with its contractual obligations regarding the confidentiality of information it receives from third parties.

3. LP may disclose Confidential Information only in accordance with the LPCOP.

As LP is part of AXP, it is generally acceptable for LP and the rest of the AXP group to share their information, resources and business strategy.

However, LP has access to confidential and commercially sensitive information about its clients and partners, as well as personal data relating to its customers, which must be treated carefully and may only be disclosed to other business units in AXP on a restricted basis. This includes disclosure to other divisions of GMS & GLC and any other AXP line of business and staff group areas.

Conversely, LP must not disclose confidential or commercially sensitive information which it receives relating to AXP to any third parties, including partners and customers of LP except as permitted in accordance with applicable AXP policies.

The general principle is that Confidential Information may only be disclosed to AXP business units outside LP where it is required for a legitimate business purpose and on a 'need to know' basis. Application of the LPCOP principles set out below will ensure compliance with this principle.

3.1 LPCOP Principle 1

LP must comply with all applicable laws and regulations on the sharing and use of information it holds.

The two primary areas of regulation that restrict the ability to share Confidential Information are competition law and data protection law. Other areas of regulation may also apply and will be taken into consideration by the Network Information Control Officer as part of the review under the LPCOP.

3.1.1 Competition Law Rules

In some business areas, some partners or clients of LP may be considered an actual or potential competitor of AXP. The exchange of ***commercially sensitive information*** between competitors is prohibited under competition law as this may distort and undermine competition in the market. Violations of competition law can have serious financial and reputational impacts for companies and can even lead to imprisonment for individuals who facilitate violations.

In the context of LP's business, potential competitors to AXP would include, for example:

- ***Issuing banks*** who offer LP co-branded payment cards (whether Visa/MasterCard cards or American Express cards under a GNS license) or who use LP as a distribution channel for their card-related services, which compete with cards issued by Proprietary Card Services (PCS);
- ***Insurance companies*** who distribute insurance in competition with International Insurance Services (IIS); and
- ***Travel agencies who*** sell and book travel in competition with Global Business Travel (GBT) or consumer travel units with PCS, such as Travel and Lifestyle Servic*es* ***(TLS).***

Please note, that this is not an exhaustive list.

Commercially sensitive information would include, for example, prices and rates agreed with customers or partners, performance results and marketing and business strategies and plans.

To name some specific examples, the following types of information would be commercially sensitive:

- ***Prospective issuing partner*****:** LP negotiates with a non-proprietary issuer regarding the issuer's prospective participation in a LP loyalty program. This also involves a simultaneous negotiation between the issuer and GNP regarding an American Express card issuing license. The existence of both of these negotiations (LP and GNP), as well as any terms under negotiation, including the timing or launch, would constitute commercially sensitive information.

- ***Established issuing partner***: A non-proprietary issuer of American Express cards is an established partner in an LP loyalty program. As part of its participation in the program, metrics regarding the issuer's performance in the program are held by LP. This would very likely constitute commercially sensitive information (and even if it does not, under the confidentiality terms of LP's contract with the partner, it would likely still qualify as Confidential Information for purposes of this policy more generally).

- ***Insurance distributor*****:** An insurance company underwrites white label insurance that is marketed under the brand of an LP partner. The partner seeks to market the insurance, or provide points to LP customers who purchase an insurance. AXP's IIS unit distributes insurance in the same market. Any non-public commercial terms under which such insurance will be marketed or incented, including the timing of an upcoming launch for any such marketing or bonus campaign would be commercially sensitive information.

To ensure compliance with competition law, LP must take care to ensure that commercially sensitive information relating to partners or clients of LP which could be said to compete with any AXP business unit

must not be disclosed to the relevant AXP business unit. This constraint applies even if there are no contractual restrictions on the disclosure or use of this information.

In all of examples given above, LP staff should not share the information under any circumstances with persons responsible for managing the relevant competing AXP business (e.g. PCS, IIS and TLS, respectively).

It is possible for an AXP employee with responsibility for a business unit that competes with an LP partner to sit on the board of an LP legal entity. It is also possible for both an AXP business unit and a competing LP partner to be partners in an LP program and involved in meetings of partners. However, in these cases special precautions must be taken as outlined in the LPCOP Governance Procedure below. Finally, even more generally, LP staff should not share commercially sensitive information freely with other AXP employees even if they are not responsible for managing a competing AXP business. Such information should only be shared with AXP employees on a 'need to know' basis in support of a legitimate purpose, for example, managing Blue Box-wide risk management in relation to partners. For the avoidance of doubt, commercially sensitive information relating to AXP may never be disclosed to competing partners or clients of LP. Disclosure to others is also prohibited except in rare circumstances and within tight controls in accordance with relevant AXP policies.

*Before disclosing any **Confidential Information**, you must first confirm that the information does not relate to a company which could be said to compete with AXP and that the information is not commercially sensitive. Please consult the Network Information Control Officer in accordance with the LPCOP Governance Procedure.*

3.1.2 Data Protection Law

Data protection laws place restrictions on the disclosure and use by a business of personal information regarding individuals which it has collected or received, such as names, addresses, telephone numbers and shopping history.

This information is referred to as **Personal Data** or, within AXP, as personally identifiable information (PII).

Generally, data which is anonymized or aggregated (i.e. where the data of any specific individual cannot be identified) does not constitute personal data.

Whether it is permissible to disclose Personal data will depend on the extent of the disclosure statement in the relevant contracts. LP customer and employee contracts do not generally allow the transfer of Personal Data within AXP for use by other business units. In addition, apart from contractual disclosures, data protection law itself may in some cases limit transfers and use of Personal Data within the AXP group. It is therefore unlikely that Personal Data can be disclosed.

However, there may be exceptional circumstances where it may be possible to do so. This can only be assessed on a case by case basis and must be pre-approved by the Network Information Control Officer in accordance with the LPCOP Governance Procedure.

*Before disclosing any **Personal Data** outside LP, you must confirm that the Personal Data is anonymized or aggregated or can otherwise be disclosed under data protection rules. Please consult the Network Information Control Officer in accordance with the LPCOP.*

3.2 LPCOP Principle 2

LP must comply with its contractual obligations regarding the confidentiality of information it receives from third parties.

In addition to laws and regulations that restrict the ability of LP to share Confidential Information, the contractual terms that LP agrees with its partners, clients and customers may also limit the ability to share Confidential Information or use it in a particular way.

Confidentiality terms agreed between LP and its partners, clients and customers generally restrict the disclosure of information (in particular business data, personal data, key performance indicators and contracts) to any third parties which are not specifically involved in the fulfillment of contractual obligations of LP; nor can such data be used for purposes other than LP's services. In many cases these restrictions will apply to other companies in the AXP group.

LP must honor its confidentiality agreements and contracts with its clients, customers or partners.

Before disclosing any Confidential Information outside LP, you must confirm whether there are any ***contractual restrictions*** *on the disclosure or use of the information and their scope. Please consult the Network Information Control Officer in accordance with the LPCOP.*

3.3 LPCOP Principle 3

3.3.1 LPCOP

LP may disclose Confidential Information only in accordance with the LPCOP.

The disclosure of Confidential Information must be pre-approved by the Network Information Control Officer, who will retain a record of questions and answers relating to the LPCOP.

Confidential Information about partners, clients or customers may only be disclosed to other business units in AXP in accordance with the following **LPCOP**:

1. Any requests for LP information from a non-LP AXP employee must be directed to the employee's counterpart within LP.

2. The relevant LP employee must submit this request, or a request of his or her own to share LP data with another AXP business unit, to the Network Information Control Officer at lpcop@loyaltypartner.com.

   The request must include the following information:
   - the exact nature of the information to be disclosed;
   - the name and role of individuals who will have access to the information requested;
   - the purpose for which the information will be used; and
   - whether there is any reason why the information should not be disclosed.

3. The Network Information Control Officer will provide approval or revert with additional questions. If the request is related to Personal Identifiable Information (PII), the Network Information Control Officer will consult with the local Market Data Protection Officer. If there is doubt as to whether the proposed disclosure of information is compliant with the LPCOP, the matter may be referred to a broader review team consisting of AXP's Senior Counsel - Competition Law (currently Katerina Soteri) and the AXP Market Compliance Officer for the relevant market.

4. The relevant LP employee will communicate the Network Information Control Officer's decision to his or her counterpart at the relevant AXP business unit.

3.3.2 Responsibilities of LP employees before disclosure of Confidential Information

Before any Confidential Information is disclosed to another AXP business unit, the LP employee must:

1. Establish the exact nature of the information to be disclosed, who will have access to the information and for what purpose the information is requested.

2. Evaluate whether the information to be disclosed is subject to confidentiality under relevant either regulatory or contractual obligations.

3. Conspicuously mark the Confidential Information to be provided as CONFIDENTIAL.

4. Follow the LPCOP.

5. Ensure that the recipient confirms the following points in writing (e.g. by email) to the Network Information Control Officer and the LP employee:
   - that the recipient have reviewed the LPCOP;
   - that the recipient will not disclose the Confidential Information to anyone else without the prior approval of LP; and
   - that the recipient will not use the Confidential Information any other purpose without the prior approval of LP.

3.3.3 Circle of trust

In deviation from principle 3.3.1 where each disclosure needs to be approved on a case-by-case basis, LP has installed a so called “Circle of Trust”. Members of the Circle of Trust can only be nominated by the LP staff departments, i.e. tax, controllership / accounting, finance, GCO. The request for the nomination as member of the Circle of Trust must include the following information:

- the exact nature of the information to be disclosed;
- the name and role of individuals who will have access to the information requested;
- the purpose for which the information will be used; and
- whether there is any reason why the information should not be disclosed.

The members of the Circle of Trust have to abide by the rules of section 3.3.2, however once admitted to the Circle of Trust, information otherwise restricted by LPCOP can be transmitted to them on a regular basis, without renewal of verification, for as long as required. In case of a change in responsibility of the respective member of the Circle of Trust, the LP contact person of the staff department shall inform the Network Information Control Officer accordingly, so that the respective person can be excluded from the Circle of Trust.
In any case, the list of members of the Circle of Trust shall be updated on a yearly basis at the beginning of each calendar year.

3.3.4 Membership of AXP employees in LP boards or in LP senior management

In situations where an AXP employee with direct responsibility for an AXP business unit that competes with an LP partner also assumes responsibility as a board member or director of an LP legal entity, the following steps must be taken:

1. The Network Information Control Officer in the Compliance Team must review the agenda of any board meeting, and any materials distributed to board members, in advance of the meeting.

2. If it is necessary for the board to discuss matters that involve the Confidential Information of the relevant partner, the AXP representative must leave for that portion of the meeting.

3. Minutes of any meeting touching on Confidential Information of a competing partner or client must be free from references to Confidential Information and should be reviewed by the Network Information Control Officer before distribution to board members.

4. Where possible, business performance metrics provided to the board should be provided using a standard template form approved in advance by the Network Information Control Officer.

3.3.5 AXP employees and competing business partners

In situations where an AXP business unit and a competing LP partner are, by virtue of their partnership status in the LP program, contributors to the core partner group (e.g. Platinum partner meetings), or where two non-AXP LP partners are competitors (e.g. two food retailers, or two bank card issuers) and members of the core partner group, the following steps must be taken:

1. The Network Information Control Officer must review the agenda of any group meeting, and any materials distributed to group members, in advance of the meeting to ensure these are free from any Confidential Information of either competing partner.

2. The sharing or discussion of Confidential Information of either competing partner among the members of the partner group is strictly prohibited.

3. Any agreement - formal or informal, direct or indirect – between competing partners on competitively sensitive matters (e.g. pricing, customer allocation, commercial strategy, blocking competitors) is strictly prohibited.

4. Minutes of partner group meetings must be reviewed by the Network Information Control Officer before distribution to member partners; and

5. The Network Information Control Officer will draft constitutional documents of the group to incorporate this procedure and prohibit generally the sharing or discussion of Confidential Information of competing partner and / or the discussion or agreement of competitively sensitive matters among competing partners. The constitutional document must be approved and adopted by the group.

6. Where possible, performance metrics provided to the partner group should be provided using a standard template form approved in advance by the Network Information Control Officer.

4 EXCEPTIONS

Specific exceptions may apply in accordance to existing contract agreements between LP, its partners and AXP. For any exception requests not covered in this section, please contact lpcop@loyaltypartner.com. For the avoidance of doubt, LPCOP principles 3.3.2 and 3.3.3 shall apply for such exceptions nevertheless.

4.1 Mexico

a) For the case of Payback Mexico, information may be shared between LP and AXP based on intercompany agreements and only for the services render such as:
   - Analytics
   - Customer Services to MR customers
   - Fraud.

4.2 Italy

a) For the case of Payback Italia, information may be shared between LP and AXP based on intercompany agreements and only for the services render such as:
   - Analytics
   - Customer Services to MR customers
   - Fraud

4.3 US Plenti (Amex Travel Related Services Company, Inc.)

a) For the case of Plenti, information may be shared between LP and AXP based on intercompany agreements and only for the services render such as:
   - Analytics
   - Customer Services to MR customers
   - Fraud

5 RELATED POLICIES, REGULATORY GUIDELINES AND SUPPORTING DOCUMENTS

This policy must be read in conjunction with the following policies and regulatory requirements:

- The American Express Information Security Policies and Standards Library
- American Express Management Policies (AEMP)
- AXP Code of Conduct
- Local Market Anti-Trust Law Requirements
- Local Market Competition Law Requirements

6 REVISION HISTORY

- First Publication November 2011
- Second Publication November 2013
- Third Publication July 2016

7 APPENDIX

7.1 Examples of partner confidential information

PARTNER INFORMATION	Disclosure to 3rd Parties* Generally	Disclosure to 3rd Parties* under NDA	Disclosure within AXP Generally
Names, industry and country of established partners	Yes	Yes	Yes
General benefits for partners of LP	Yes	Yes	Yes
General partnership model	Yes	Yes	Yes
Best practices	Yes	Yes	Yes
Partner specific program data, e.g.: • Transaction volumes • Collector registrations • Customer statistics • Revenue uplift • Marketing data such as response rates, business impacts • Results of promotions	No, unless anonymized and aggregated across partners leaving no ability to discern any individual partner data, even when combined with other data available elsewhere		
Standard partner contract terms	No	Yes, in the context of a negotiation with a prospective partner	Yes
Partner-specific contract terms	No	No	No, unless approved via LPCOP No, to competing AXP business unit
Existence of negotiations with named specific partner	No	No	No, unless approved via LPCOP No, to competing AXP business unit
Financial and commercial data that is publicly available, e.g. through internet, commercial registry, etc.	Yes	Yes	Yes
Financial and commercial data that is not publicly available, e.g. through internet, commercial registry, etc	No	No	No, unless approved via LPCOP No, to competing AXP business unit
Other potential Confidential Information	Consult with Network Information Control Officer		

**Third parties other than those competing with a partner and, in all cases, with a legitimate business purpose*