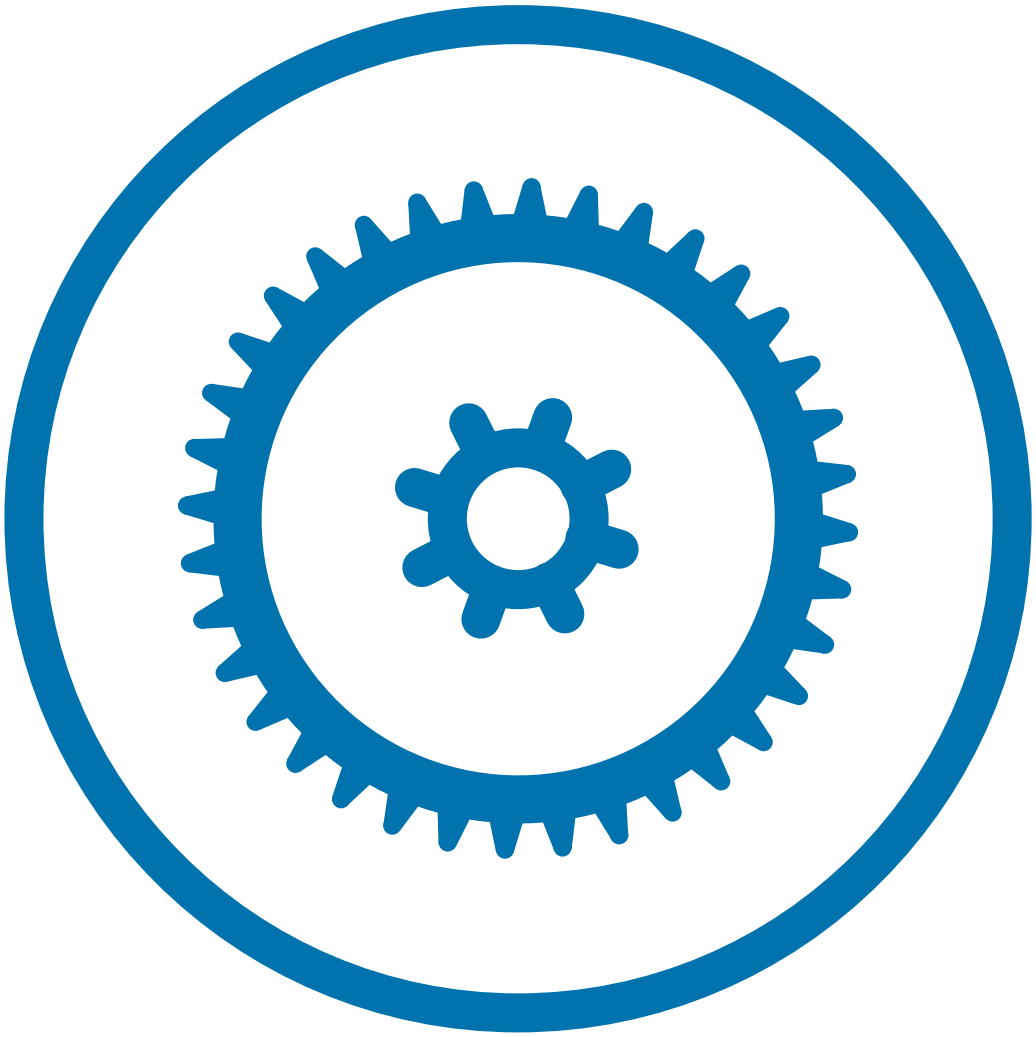
Position Paper

protection of privacy in card-linked offers



worldline
e-payment services

an atos company

Protection of privacy in card-linked offers

The use of big data creates tremendous business opportunities that benefit data providers (payment card issuers, acquirers and merchants) and end users alike.

In this context, card-linked offers seem very promising, as people are now willing to try out new types of digital services, as shown by the recent advent of such initiatives in Europe.

However, even though they interact with technology more than ever before, people are also more worried about their personal data. Actually, seven Europeans out of ten are concerned about how companies might use the information that they disclose, and 54% of people are also particularly wary about the use of their payment card data[1].

Indeed, handling personal data remains a sensitive task because of regulatory, image and security issues. Regulations also change quickly in this domain, and keeping up with them is not easy. A data provider's image can be hurt if the regulatory declaration and public announcement concerning data use are not carried out perfectly, or if private data are leaked because of security breaches.

Regulations

Card-linked offers use personal data, which are defined as any information related to an identified or identifiable natural person. The processing and transfer of such data are regulated by European and national rules.

With the ever-growing use of private data for business purposes, regulations have to adapt constantly to protect natural people's privacy.

Today, in the European Union, data protection directive 1995 95/46/EC has been transposed into member states' legislations, but sometimes with national specifics. However, the upcoming European General Data Protection Regulation (GDPR) proposed by the European Commission will be directly applicable to all EU member states without any transposition into national laws, and organizations are expected to comply with this regulation two years after the vote.

Before private data may be used for business purposes, national regulations require that information or declaration files be supplied, depending on countries.

Parties' responsibilities and reliability

As far as regulations are concerned, a distinction is made between controller, processor, third party and recipient. Controllers (Issuer, Acquirer or Card-Linked Offer entity) are responsible for the use of the data, and they legally have to either declare this use or inform regulatory organizations about it.

Controllers must ensure that their card-linked offer processors guarantee the compliance and security of the use of private data. A highly reliable experience and contractual agreement are key elements for this purpose.

Concern over public reaction

Recent examples have demonstrated the negative effects of badly prepared communication about data handling.

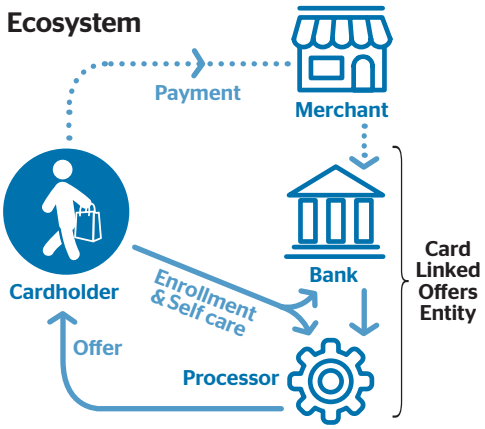
Various country cultures and philosophies emerge in national data privacy legislations as well as in the data uses that people accept. These elements have to be taken into account and dealt with very seriously in public communications.

In each country where the concept of card-linked offer is new, public communication has to be organized specifically and carefully.

Definition of a card-linked offer

A card-linked offer is any offer that can be linked to a card and redeemed, generally through cashback.

Card-linked rewards use transaction data and other data to provide consumers with relevant offers that are delivered through digital channels and which can be credited directly to the consumer's payment card/account. Redemption is automatic at the point of sale.



Meet regulatory requirements

Today, regulations have specifics in each country; however, the main principles are common, in accordance with the OECD's recommendations.

In European countries, the upcoming GDPR regulation is already the reference for personal data protection and privacy clauses in contracts.

Cardholder's consent

In the European context, it is necessary to obtain the cardholder's consent before collecting and using their private data.

The cardholder's consent should be obtained explicitly, and must not be hidden in "Terms of use" text. The terms used to obtain the user's consent must state explicitly:

- which data are collected,
- the purpose of the data collection,
- how the data are disclosed,
- who collects the data,
- the identity of the data recipient,
- how opposition or modification rights can be exercised.

The new European GDPR rules will also put citizens back in control of their data, notably by granting them the right to be forgotten.

Obligations

For controllers and their partners, the main obligations in terms of data management are:

- the data retention time must be limited and adapted to the purpose of the data collection.
- the data must be kept up-to-date.
- the data storage and processing locations, and data transfers depend on countries' regulations.
- the collected data must be protected, and data damage, alteration, leaks or access by unauthorized people must be prevented.
- data disclosure must be declared.

Regarding data use, the data analysis carried out to create the cardholder's profile must not deprive people of a good or service (for instance, a cardholder who often goes to drugstores must not be deprived of health insurance coupons).

Database interconnections (relationships between data that were initially distinct) are also fully regulated and require specific authorizations in some cases.

1 *Flash Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union - June 2011.*

Legal formalities

These formalities have to be taken care of by the data controller of the program, which is the Issuer or Acquirer.

Today, depending on countries, legal formalities can consist in declaring the data use to national authorities or simply informing them. These rules will be harmonized when the GDPR becomes applicable[2]. The procedure for declaring data use to a national authority can take from 4 months to 1 year depending on the country and the complexity of the case.

Lack of compliance with existing regulations might result in sentences, penalties and also public communications that could hurt the data controller's reputation and brand image.

Fulfill responsibilities and reliability to create trust in data

The security and privacy of the data are also crucial requirements for customers to accept card-linked offers.

Security is fundamental to avoid personal data breaches. Some recent attacks that have had a huge impact on certain brand images have also shown that criminal organizations get smarter when it comes to hacking into systems. Banks' expertise and experience in security are recognized by the market; this is why banks should take advantage of these assets in the business of card-linked offers.

For banks, privacy already exists. Nowadays, banks should go further by empowering their customers in order to make the bank-customer relationship more balanced. For instance, customers are likely to choose for themselves the intended data use, and who is allowed to access their account data and private data.

Both security and privacy are needed to create trust, and for card-linked offers to be successful.

Achieve security

A high level of security is required to prevent private data breaches that might considerably jeopardize the success of the program. Some advice to achieve such security is:

- secure access within organizations,
- restrict access to private data,
- anticipate the risk of data loss,
- anticipate the fraudulent use of coupons,
- educate staff about security.

Cardholders are also required to use strong passwords to protect the access to their profiles and cashback funds requests. PCI-DSS compliance is mandatory when processing card-linked offers since card payment data are handled in the process. When working with third-party processors, tokenization is a way of achieving PCI-DSS compliance effectively.

Achieve privacy

Privacy Impact Assessments (PIAs) is a process whereby organizations identify and reduce the risks of data handling, and define an appropriate way of achieving privacy. One of the main advantages of PIAs is that privacy principles are an integral part of the service and personal data processing.

Card-linked offers should also embed Privacy by design i.e. they must contain built-in personal data protection mechanisms as of the design of the solution and throughout the life cycles of technologies and procedures.

Anonymization of cardholder identity is a key challenge of a card-linked offer program. Cardholder identity must be anonymized within the Data analytics module, but to communicate with the cardholder, the token must remain related to the real enrolled identity, e-mail address and/or mobile number of the cardholder.

Minimal disclosure technologies could also be possible solutions to achieve effective personal data protection, as they enable users to minimally disclose certified information about themselves. These innovative cryptographic technologies provide strong privacy protection by offering superior user control and preventing unwanted user tracking (e.g. Attribute-Based Credentials).

All ecosystem players must comply

When elaborating a card-linked offer service, banks must ensure that all the partners of the ecosystem meet all security and privacy requirements: processors, banks' internal IT systems, merchants, program administrators.

Therefore, your potential partners, including your third-party processors, should be selected according to several key criteria such as:

- experience, reliability and critical size,
- ability to conduct projects, including security and tools for identifying and reducing privacy risks beforehand,
- international presence needed to handle the widest range of national requirements and regulations.

Manage public concerns

With card-linked offers, the concerns pertaining to data privacy and personal information security could prove higher than for any other couponing program, since card transaction data are used.

These concerns should not be ignored or hidden. Banks must prove to customers and the public that they excel at handling data with extreme care at all times. This prevents disproportionate reactions from the press, social networks, politicians and consumer associations that may arise in this new digital context.

Communication

Data protection and privacy should be the top priority of your communication. Any communication (e.g. press releases, social network posts, or radio and TV broadcasts) must always mention privacy measures, and the message has to be clear enough so people can assimilate it easily.

Bank staff and call centers agents have to be educated so they are capable of answering questions about the features of card-linked offers without omitting to reassure people about their compliance with privacy requirements.

Banks have also an exceptional position on trust matters. They must make the most of this advantage to extend their clients' trust to card-linked offers and new digital propositions.

Apprehensions to overcome

The transfer and sale of data to third parties are not yet accepted by the general public[3]. Therefore, they must not be considered in business perspectives today, and communication must insist on this fact.

Geolocation is still a special feature, as opinion polls reveal that only 25% of the people would be ready to accept it.[4]

Data location also worries people. Even though regulations authorize cross-border data transfers under certain conditions, 52% of people want their personal data to be kept on their national territories. [4]

Accelerate the change of mindset

The public opinion is more and more ready for personal data sharing, especially with banks, as 70% of customers are willing to provide their bank with more information in exchange for better services[5].

Giving cardholders the ability to manage the use of their data through self-care interfaces (profile, coupon frequency, channels, blacklisting) is also important to reinforce the cardholder's trust in the service.

Conclusion

By proposing card-linked offers, banks access a new business domain in Big Data, based on their privileged position as trusted partners.

This new field generates increasing security and privacy challenges that require investments in legal resources, security infrastructure, processes and client communication.

As card-linked offers need big volumes to build up a successful ecosystem with merchants and cardholders, creating a consortium or participating in an existing one should be considered.

Consequently, trustworthiness and business size are key features when choosing your partners and subcontractors.

These recommendations are essential to stay ahead in the digital banking competition.

2 Vote is forecasted the 1st January 2016.
3 Baromètre de la confiance des Français dans le numérique – Caisse des Dépôts et ACSEL - Vague 3.
4 Les français & la protection des données personnelles - Etude de l'Institut CSA pour Orange - Février 2014.
5 EY - Transforming banks, redefining banking - 2014.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry. Worldline delivers new-generation services, enabling its customers to offer smooth and innovative solutions to the end consumer. Key actor for B2B2C industries, with 40 years of experience, Worldline supports and contributes to the success of all businesses and administrative services in a perpetually evolving market. Worldline offers a unique and flexible business model built around a global and growing portfolio, thus enabling end-to-end support. Worldline activities are organized around three axes: Merchant Services & Terminals, Mobility & e-Transactional Services, Financial Processing Services & Software Licensing. Worldline employs more than 7,300 people worldwide and generated 1.15 billion euros revenues in 2014. Worldline is an Atos company.

Financial Processing & Software Licensing

Financial processing provides banks and other financial institutions with a comprehensive set of services to help them and their customers manage their cashless payments. Our services and innovative software solutions support the full range of card and non-card payments for acquirers and issuers. By combining our core services with a growing list of value-added services and full integration with in-house systems, we help our clients offer their customers a customised, profitable, secure, extensive and innovative product portfolio.

For further information
infoWL@worldline.com

Disclaimer

This document is intended to provide only general information, and focuses on the European scope. Do not, under any circumstances, consider this information as legal advice.