

ARTICLE 29 - DATA PROTECTION WORKING PARTY



Brussels, 11 January 2005

Subject: Guidelines for Terminated Merchant Databases

Dear Colleagues,

Please find attached the final “Guidelines for Terminated Merchant Databases” that have been negotiated between the payment industry and the Working Party over the last two years, and that were discussed at our last meeting in late November.

At our November meeting the latest version of the Guidelines was presented, and you were all invited to provide further comments with a view to finalizing the Guidelines by the end of this year. A number of comments have been received and the payment industry has produced a new version of the Guidelines that takes such comments into account. All changes from the version discussed in November are indicated in the text.

After consulting with the Commission, I have examined these changes and I am of the opinion that they adequately address the questions and comments received. While the Guidelines remain in the nature of best practices and apply without prejudice to the provisions of the applicable national legislation, I believe that these Guidelines provide a satisfactory protection for data subjects and that their use will increase the level of personal data protection for terminated merchant databases. I further believe that the Working Party’s endorsement of documents such as this can provide an important mechanism for addressing data protection issues in particular sectors in a timely and yet effective fashion.

Based on the above, I hereby endorse the final version of the Guidelines as attached. I have therefore asked that these Guidelines be officially published on the website of the Working Party together with this letter. The Working Party shall then monitor their implementation by the payment industry, the review of the Guidelines being scheduled in early 2006.

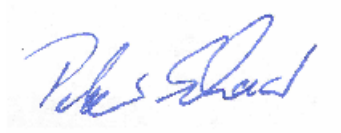
The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC. The Secretariat is provided by:

Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

I would like to thank you all for your contribution in the drafting of this document and, in particular, those who volunteered to participate in the meetings of the sub-group which contributed in this important effort.

Sincerely yours

A handwritten signature in blue ink, appearing to read "Peter Schaar", is centered below the text "Sincerely yours". The signature is written in a cursive, flowing style.

The Chairman
Peter Schaar

Guidelines for Terminated Merchant Databases

December, 2004

I. Introduction

These Guidelines are designed primarily as an instrument of best practice, and are intended for use as a reference document within the framework of applicable laws. They set forth the conditions under which payment systems, banks, payment services providers, associations, and other participants (all referred to herein collectively as the “Participants”) may operate cross-border databases containing the data of merchants which have been terminated from participating in their systems or the systems of their members based on objective criteria related to specified irregularities and/or risks, (hereinafter referred to as “Terminated Merchant Databases”). The document applies to all such databases run whether bilaterally, multilaterally, or otherwise by two or more Participants established on the territory of one or more EU Member States. Various such databases exist or are presently being developed at the international, regional, and bilateral levels. Such databases do not contain “sensitive data” within the meaning of Article 8 of Directive 95/46/EC, but are designed to reduce payment fraud, which the Commission identified as a priority in its Action Plans issued in February 2001¹ and October 2004².

¹ Communication from the Commission "Preventing fraud and counterfeiting of non-cash means of payment", COM (2001) 11 final of 9 February 2001, available at: http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/index.htm.

² Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol “A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment”, COM/2004/0679 final of 20 October 2004, available at: http://www.europa.eu.int/comm/internal_market/payments/fraud/index_en.htm.

³ The exclusion of data relating to offences, criminal convictions and security measures from the database implies among others that no data referring to judicial and administrative litigation shall be processed and that only objective facts related to the merchants and the reasons for their termination shall be processed exclusive of any data of a subjective nature such as suspicions and rumours.

⁴ Four-digit classification codes used in authorization, clearing, and other transactions or reports to identify the type of merchant. Also referred to as merchant category code (MCC).

⁵ CAT is a magnetic stripe or chip reading terminal (usually unattended by a merchant representative) that dispenses a product or provides a service when activated by a

Participants commit to operate the databases under the standards laid down in the Guidelines, subject always to their obligation to comply with relevant national laws applicable pursuant to Article 4 of Directive 95/46 which may require a slightly higher level of protection, or their self-regulatory provisions. The Guidelines are not intended to reduce or replace the applicability of national laws and regulations, including any applicable exceptions or exemptions.

Participants should already be dedicated to respecting data protection laws, and should have measures in place to ensure compliance with them. In order to ensure a more uniform application and interpretation of some of the provisions of Directive 95/46 and national laws implementing it, the Working Party subgroup decided at its meeting of 4 June 2004 to have draft guidelines prepared on terminated merchant databases (hereinafter referred to as the “Guidelines”).

The Guidelines clarify the application of national implementing measures in order to contribute to their uniform application throughout Europe, without amending them, in order to increase legal certainty for individuals, data protection authorities, and Participants. They are intended to provide basic protection for personal data in databases in which terminated merchants are included.

The Guidelines will be applicable to any processing activities in the framework of a terminated merchant database by a Participant established on the territory of an EU Member State with respect to merchants established in an EU Member State. They are to be adopted by Participants so that the principles contained therein are legally binding on them. The responsibilities of the Participants are summarized at the end of the Guidelines.

The Participants recognise that the Guidelines are not a substitute for compliance with all legal requirements in all Member States and that further steps might need to be taken on the national level. The Guidelines also do not prejudice any *ad hoc* negotiations at national level.

The Guidelines will be reviewed twelve months after their adoption. Further work on the specific area of international data transfers will be carried out in consultation with the Article 29 Working Party Subgroup on International Transfers.

All provisions of these Guidelines apply without prejudice to the provisions of the applicable national legislation. Where specific requirements exist at national level, they will have to be complied with in accordance with the applicable rules set out in these Guidelines and in accordance with EU legislation.

II. Guidelines

Terminated Merchant Databases must meet at least the following standards:

1. **Legal grounds:** The processing shall comply with the requirements of Article 6 of Directive 95/46/EC and be based upon one or more of the legal grounds specified in Article 7 of Directive 95/46/EC. Such legal grounds may differ depending on the applicable Member State law and may include (depending on the applicable Member State law) consent of the individual; that the processing is necessary for compliance with the specific legal obligations (i.e., to prevent fraud) to which the data controller is subject according to the relevant legal framework; that the processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for the fundamental rights and freedoms of the individual; or other grounds provided for by national law.
2. **Parties and data covered:** The database shall only contain data identifying terminated merchants with information on their principal owners, and shall not contain data identifying individual cardholders. “Sensitive data” within the meaning of Article 8 of Directive 95/46/EC (including information concerning offences, judicial data, criminal convictions and security measures³) shall not be included. Data included shall be sufficient to identify the merchants entered in the database as allowed by applicable law.
3. **Purpose limitation:** Use of the database shall be strictly limited to processing data about terminated merchants for the purpose of allowing Participants to analyse the risks associated with signing up a particular merchant. The data shall not be used for any other purpose.
4. **Information and transparency:** Information about the database and the rights of merchants listed in it shall be provided to merchants in an open and transparent manner and as provided for in the applicable national data protection laws and regulations. Information may be made available via layered notices as foreseen in the Working Party’s “Opinion on More Harmonised Information Provisions” (WP 100) of November 25, 2004. A mailing providing information about the database in an open and transparent manner shall be sent to all current merchants. New merchants shall be informed in an open and transparent manner about the database in their contract with a Participant when they are initially signed up. Information may also be published in major newspapers if this is found necessary in a particular case. At the same time that they are informed about their termination, all merchants shall be informed about their inclusion in the database and about the rights they can exercise under applicable data protection legislation (e.g., right of access, rectification, and complaint).
5. **Relevancy and proportionality:** The database shall be limited to objective information which would enable a Participant to (i) identify unambiguously a particular merchant and its principal owners, (ii) identify the reason(s) for which such merchant has been terminated and, subsequently, (iii) evaluate the risks associated with signing up such merchant. Appendix 1 contains a description of the data fields

typically contained in the database. Such information may vary based on local practice and legal requirements. Any additional comments must be accurate, objective, and relevant, and must comply with the rules set forth in these Guidelines. Inclusion in the database shall be limited to merchants who have been excluded or terminated from the payment system based on objective criteria.

6. **Accuracy:** Steps shall be taken to ensure that the data is accurate and kept up to date. In particular, the Participants that enter information into the database must take measures to ensure that the data entered is accurate, and the Participants responsible for maintaining and operating the database (the “Database Operators”) must correct any reported inaccuracy of the data in the database to the best of their ability. Every reasonable step shall be taken to ensure that data which are inaccurate or incomplete are erased or rectified, having regard to the purposes for which they are collected or further processed. Appendix 2 contains a description of the typical measures to ensure the accuracy of the data.
7. **No automatic decision making:** The decision to include a particular merchant in the database shall be subject to supervision by trained staff, and shall not be based solely on automated processing of data. Likewise, inclusion in the database shall not be a basis for automated decision-making; i.e., if a merchant is listed it shall still be up to the discretion of another Participant as to whether to sign up that merchant.
8. **Sensitive data:** The database shall not include “sensitive data” within the meaning of Article 8 of Directive 95/46/EC. In particular, the database shall only contain objective factual information related to irregularities commonly addressed by Participants as a risk factor, and shall not contain rumours and mere suspicions.
9. **Onward transfers:** Access to the database shall be strictly limited to Participants that are bound by the terms of use of the database including the present Guidelines, except where otherwise required by a court order or any administrative or legal requirements of national or international applicable legislation which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC (such as tax or anti-money-laundering reporting requirements). Participants (other than Database Operators, who require full access in order to operate the database) shall only be given selective access to the database to verify whether it contains any input about a specific merchant that has applied to become a member of the system. Data in the database shall not be shared with other entities or services of the Participants for other purposes. The merchants must be given information about any onward transfers in the informational notices (see above – “Information and transparency”).
10. **Rights of individuals:** Merchants whose data are included in the database have rights of information, access, rectification and objection, and to obtain compensation in case of suffered damage with regard to the uses of their data. The foregoing shall be without prejudice to the contractual arrangements between the Participants as to their respective liability vis-à-vis each other. In case the inclusion of a merchant is

disputed, it may be more convenient for the merchant first to apply to the Participants with which it had a direct contractual relationship, but the merchant may always apply as well to any of the other data controllers of the database. A merchant's data shall be immediately deleted from the database if it is found that such merchant's inclusion was not in accordance with the requirements that apply to the database, and parties that had accessed the relevant data within the previous twelve months shall be promptly notified of the deletion. These protections apply to legal entities as well in those Member States that cover legal entities in their data protection law.

11. **Data retention:** The Database Operator shall delete data on expiration of the period allowed by relevant national legislation, and in any case when it is no longer needed for the above-mentioned purposes, or after five (5) years at the latest (or whatever other maximum period as provided for under national law), unless retention for a longer period is necessary for the assertion of legal claims or to meet specific legal obligations.
12. **International transfers:** The data in the database may be transferred outside the EU only when it is authorised under Articles 25 or 26 of Directive 95/46/EC or based on any other grounds provided for by national law, and solely for fraud prevention purposes. Access to the database in third countries shall be limited to Participants that are bound by the terms of use of the database.
13. **Security:** State-of-the-art security measures shall be implemented to ensure the security of personal data in the database. This shall include appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, as well as the completion of regular internal audits.
14. **Dispute resolution:** Appropriate dispute resolution mechanisms shall be made available to merchants in order to resolve disputes about their inclusion in the database. In most cases, it is advisable for the merchant first to inquire with the Participant that it had a contractual relationship with. That Participant is contractually bound to deal with the merchant to attempt to resolve any such dispute. At any time the merchant may also address any inquiries to the Database Operators, which will have a data protection officer who will help to clarify such inquiries. If the data protection officer finds that the merchant has been listed in the database incorrectly, then it will order the merchant's name to be removed and the merchant will also have all the other rights outlined in the Guidelines. Appendix 3 provides an example of appropriate procedures to exercise individuals' rights including an adequate dispute resolution procedure. A merchant of course always has the option of complaining directly to the relevant data protection authority or other authorities. Dispute resolution procedures shall reflect the rights of individuals as described above (see above – "Rights of individuals").

15. **Deadlines:** The Participants shall undertake to modify their systems to comply with these Guidelines within twelve (12) months of their adoption.

16. **Parties' Responsibilities:** The development and operation of a terminated merchant database require the joint action of two Participants acting as joint data controllers for any particular set of personal data relating to a specific merchant, namely 1) the Database Operator, and 2) the Participant that has a contractual relationship with the merchant.

The following is a brief summary of these parties' responsibilities under the Guidelines:

Provision	Responsibilities	Responsible Party
Information and Transparency	Providing information to merchants in a mailing	Participant that has a contractual relationship with the merchant
	Providing information upon termination	Participant that had a contractual relationship with the merchant
	Publishing information in major newspapers (when necessary)	Participant that had a contractual relationship with the merchant
Accuracy	Accuracy upon entering data in the database	Participant that had a contractual relationship with the merchant
	Maintaining accuracy of the Database (including updates)	Participant that had a contractual relationship with the merchant; Database Operator(s)
Rights of individuals	Responding to merchants' request to exercise their rights	Participant that has a contractual relationship with the merchant; Database Operator(s)
	Deletion of data, and notification of Participants that had accessed it within the last 12 months	Database Operator(s)
Data retention	Deletion of data after expiration of retention period	Database Operator(s)
Security	Implementation of security measures	Participant that had a contractual relationship with the merchant; Database Operator(s)
Dispute resolution	Working with merchants to resolve disputes	Participant that had a contractual relationship with the merchant; Database Operator(s)
	Deleting improper listings	Database Operators
Deadlines	Implementation of measures within twelve months	Participant that has a contractual relationship with the merchant; Database Operators

APPENDIX 1

Illustrative Data Fields and Reason Codes

Note that all this information is illustrative, and may vary based on local law and conditions.

A1. Data Field Examples (mandatory or optional)

Merchant data:

- **Unique Transaction Identifier** (the acquirer's Bank Identification Number (BIN), Request Date, Locator Number, Sequence Number, Action Indicator, and Agreement reference number)
- **Acquirer Country Code**
- **Merchant Country Code**
- **Merchant Trading Name/DBA**
- **Merchant Legal Name** (the parent or holding company name must be entered if this name is different from the Merchant Trading Name/DBA)
- **Merchant Street Address**
- **Merchant City**
- **Merchant Province Code**
- **Merchant Postal Code**
- **Merchant Telephone Numbers**
- **Merchant Category Code (MCC⁴)**
- **Merchant Bank Account Number (including branch identifier)**
- **Value Added Tax Number/Merchant Identification Number** (merchant's national/State VAT identification number)
- **Listing Reason Code**
- **Chamber of Commerce registration number**
- **Contract Opened Date** (the date the merchant contract was opened)
- **Contract Closed Date**
- **Indication whether the merchant uses cardholder-activated terminals (CAT)⁵ or not**
- **Commercial name by which the merchant is known**

Principal owner data:

- **Principal owner's identity** (last name, first name and middle initial) (up to four principal owners)
- **Country code**
- **Home address of the principal owner**
- **Principal owner's phone number**

- [Principal owner's national identification number or other identifying number]⁶;

⁶ Provides more accurate identification of an individual but is only to be used if allowed by local data protection legislation.

⁷ Provides more accurate identification of an individual but is only to be used if allowed by local data protection legislation.

- [Principal owner's driver's license number / identification document number (with indication of the State that issued the principal owner's document)].⁷

A2. Reason Codes Examples

Ref. Number	Ground for listing	Comments	Definitions
01	The merchant processed irregularities (fraudulent transactions of any type, counterfeit or otherwise) meeting exceeding or the minimum objective reporting standard.	For example: - The merchant's fraud-to-sales dollar volume ratio was 6% or greater in a calendar month, and - The merchant effected 10 or more fraudulent transactions totalling USD 2,500 or more of fraudulent transactions in that calendar month. Or for example in any given month: - Three or more fraudulent transactions totalling €500, - Three or more transactions equalling 1% fraud to sales ratio; or Transactions totalling 500 which are more than 1% fraud to sales ratio.	<i>Exceeding objective reporting standard</i> is a criteria set to objectively determine fraudulent card usage at any given merchant in a given time that based upon a threshold that lies above global or European Fraud reporting averages or the Acquirer's internal criteria, whichever is more stringent. The Card Scheme membership, evaluates at global and/or European level, on a regular basis the set criteria. <i>Fraud or Counterfeit</i> Fraud or counterfeit in the context of Terminated Merchant Databases, is not to be used or interpreted in any way as a record of an offence or criminal conviction, but must only be seen as an irregularity commonly defined within the Payment Card Schemes as payment card fraud.

			<i>Counterfeit</i> The use of altered or illegally reproduced credit or debit cards (or other physical device accessing a credit or debit card account — for example, convenience checks) including the replication or alteration of the magnetic stripe.
02	The merchant was terminated for depositing sales drafts on behalf of a third party (laundering).	Laundering means that the transaction records presented by a merchant to the Acquirer were invalid for the sale of goods or services between that merchant and a valid cardholder.	<i>Laundering</i> Laundering in the context of the Terminated Merchant Databases is not to be interpreted in any way as a record of an offence or criminal conviction, but solely as an irregularity as described. <i>Sales draft</i> Paper forms cardholders use as evidence of purchases made with their card accounts; also called charge slips, sales drafts, or sales tickets.
03	The merchant was terminated because the Acquirer received an excessive number of charge-backs/Credit/Disputes due to the merchant's business practices or procedures.	The merchant's charge-backs, credits, or disputes in any single month exceeded 1% of its sales transactions in that month, and those charge-backs, credits, or disputes totalled USD 2,500 or	<i>Charge-backs</i> A dispute resolution process that members use to determine the responsible party in a charge-back related dispute. This process has three

		more. Or the Acquirer's internal criteria, whichever is more stringent.	cycles in which the members can resolve the dispute themselves. If the members do not resolve the case within three cycles, they must send the case to arbitration. These three cycles are: • First charge-back (submitted by the issuer) • Second presentment (submitted by the acquirer) • Arbitration charge-back (submitted by the issuer) <i>Disputes</i> As used herein, disputes are claims that the cardholder or another person authorized by the cardholder did not engage in the transaction.
04	The merchant is unable to discharge its financial obligation.	The merchant was terminated after it or its principal/owner was identified as prevented from continuing to trade (such as in a regulatory or administrative proceeding).	This is not to be used or interpreted in any way as a record of an offence or criminal conviction, but must only be seen as an irregularity commonly defined within the Payment Card Schemes as payment card fraud.
05	The merchant knowingly caused or facilitated, by	The merchant was terminated for being	The data is compromised while

	any means, the unauthorized disclosure, or use of account information.	identified as a single point of source of original card data used on counterfeit cards.	legitimate cardholders are undertaking a legitimate transaction. The card data is collected and transferred to an alternate (counterfeit) plastic card and used elsewhere. Alternatively, this may also occur when the card is not produced but when account data is used to undertake irregular transactions. By identifying the counterfeit card numbers and searching for the common denominator of all the genuine transactions occurred on the account numbers used fraudulently a single point of purchase or compromise can be identified. Generally within the Payment Card Schemes this practice is identified as : • Common Point of Purchase • Common Point of Compromise • Account Data Compromise
--	--	---	---

06	The merchant was in violation of a significant term or condition of the merchant agreement.	As used herein, a significant term or condition means one that concerns the truthfulness of the merchant or the commercial reasonableness of the merchant's manner of doing business that has caused or could have caused a significant risk, and does not mean a technical violation of the merchant agreement (such as one resulting in a minor financial dispute).	
07	Violation of Card Scheme Standards (the merchant was in violation of one or more of the Card schemes Bylaws and Rules manual)	As used herein, standards mean those Card Scheme operating regulations, and policies that set forth procedures to be employed by the merchant in transactions in which payment cards are used, by way of example and not limitation, honor all cards displaying the payment card mark, charges to cardholders, minimum/maximum transaction amount restrictions, and prohibited transactions.	
08	Questionable Merchant—A merchant that is the subject of an audit with respect to the Card Scheme Standards. The Card Scheme Staff currently conducts special merchant audits for excessive fraud-to-sales ratios, excessive charge-backs, or counterfeit	The reason codes apply to those merchants listed by the Card Scheme themselves (i.e. not the Acquirer). If the audit is closed and the merchant is identified as being in violation and the merchant agreement is terminated because of this violation, the merchant is	This reason is linked to objective criteria (i.e., information obtained by virtue of an audit), and does not include rumours or suspicions.

	activity.	recorded in the Terminated Merchant Database with the appropriate reason code. If the audit is closed without conclusive evidence the merchant is removed from the database.	
--	-----------	--	--

APPENDIX 2

Measures to Ensure the Accuracy of the Data

1. Responsibility

The Participants shall ensure, before entering information regarding individuals into the database, that the information is correct and compliant with data protection legislation. The Participants shall act diligently, reasonably, and in good faith to ensure the accuracy of the data and adopt strict measures to ensure the accuracy of the data. For instance, the requirements that apply to the database shall contain rules stipulating that all Participants are liable for inputting incorrect data in the database.

2. Retention of data

All personal data regarding individuals shall be securely kept for the entire duration that they are in the database.

All data shall be automatically deleted once the time limit on the retention period has expired unless it must remain available in case of a dispute on data accuracy.

3. Audit

The Participants that have a contractual relationship with the merchant shall conduct regular internal audits on the usage of the database and data accuracy.

The Database Operator can also at its discretion conduct audits on Participants to the database to ensure compliance with the requirements that apply to the database and applicable data protection legislation.

APPENDIX 3

Example of appropriate procedures to exercise individuals' rights

The following is the description of an example of procedures to exercise individuals' rights that offer sufficient guarantees to individuals listed in a terminated merchants database.

1. Access Procedure

1.1. Form of the request for access

If an individual asks a Participant whether there is any information about him or her in the database, the Participant shall explain that in order to undertake a search in the database, the Database Operator requires information in writing including the merchant's name, address, and company/business name(s).

The Participant must verify the identity of the merchant, check the name or company/business name and call the merchant in question by telephone to ascertain that the search is not being undertaken by a third party.

When the identity of the merchant is confirmed, the Participant shall send the merchant a copy of the Request for Access Form and request the individual to complete the form and sign it. The Request for Access Form is then sent to the Database Operator.

1.2. Answer to the request for access

When the Request for Access Form is returned, the Database Operator runs an inquiry on the merchant against the entries in the database.

If an exact match is found, the Database Operator sends the individual a copy of the original Request for Access Form, and a copy of the database entry. The Database Operator explains any codes or phrases which are not self-explanatory. In particular, it informs the individual of the identity of the Participant that entered the merchant in the database and the listing reason.

If no match is found, the Database Operator sends the individual a copy of the original Request for Access Form, and advises him or her that the database contains no listing which corresponds to the information provided on the submitted Request for Access Form.

If a possible match is found, but the Database Operator has reason to believe that it may not correspond to the merchant in question, it shall investigate the data elements which are different with the merchant and/or the Participant that entered the merchant in the database to ascertain whether or not it is a true match.

The Database Operator should not send out copies of database entries if it is not sure that a true match has occurred. Merchants must not be provided with listings which relate to other merchants or individuals.

1.3. Limits to the right of access

If a merchant asks whether there is any information on the database which relates to a third party, the Database Operator shall inform the individual that it can only release database records to persons who are enquiring reporting entries under their own company/business names.

2. Correction/Deletion Procedure

2.1. Form of the request for correction/deletion

Only the Participant that added the merchant to the database or the individual concerned may request that the Database Operator correct or delete the information if the addition to the database, or the information about the merchant, was entered in error.

To modify or delete a merchant listed the Participant that added the merchant to the database or the individual concerned, must send a written request by fax or by e-mail to the Database Operator. The Request for Correction/Deletion Form must contain the following information: the reference to the Participant that added the merchant to the database, the merchant name, the merchant doing business as name, merchant ID number, business address, city and state or country, principal owner, explanation for correction or deletion.

2.2. Dispute resolution procedure

If a merchant disputes being listed, the Database Operator will evaluate the request and will hear both the individual and the Participant that added the merchant to the database and based on that make a decision on the information it obtained. This decision will be motivated and communicated in writing to the individual and the Participant that added the merchant to the database. This decision is final. Individuals will retain the right of appeal in accordance with local data protection legislation.

2.3. Answer to the Correction/Deletion request

In case a correction is made by the Database Operator, the Participant that added the merchant to the database and the individual concerned will receive a Correction Response record or a printed copy of the record.

If it is found that a merchant's inclusion is not in accordance with the requirements that apply to the database, the merchant's data will be immediately deleted from the database by the Database Operator. The Participant that added the merchant to the database and the individual concerned will receive a Deletion Response record or a printed copy of the

record. The Database Operator will also promptly notify the deletion to Participants that had accessed the relevant data within the previous twelve months.