European Association
Of Payment Service Providers
For Merchants

EPSM

EPSM e.V. c/o InterCard AG, Mehlbeerenstraße 4, D-82024 Taufkirchen

EPSM e.V.
c/o InterCard AG
Mehlbeerenstr. 4
D - 82024 Taufkirchen b. München

Tel.: +49 - 89 - 6 14 45 - 412
Fax: +49 - 89 - 6 14 45 - 3412
E-mail: board@epsm.eu

**European Parliament**
**Mr Jan Philipp ALBRECHT**
**60 rue Wiertz**
**B - 1047 - Bruxelles**

by e-mail also to:

| | |
|---|---|
| LIBE Secretariat | LIBE-secretariat@europarl.europa.eu |
| LIBE Committee Members: | |
| Mr.Jan Philipp Albrecht | jan.albrecht@europarl.europa.eu |
| Mr Dimitrios Droutsas | dimitrios.droutsas@europarl.europa.eu |
| Ms Sarah Ludford | sarah.ludford@europarl.europa.eu |
| Mr Axel Voss | axel.voss@europarl.europa.eu |
| Mr Timothy Kirkhope | timothy.kirkhope@europarl.europa.eu |
| Mr Alexander Alvaro | alexander.alvaro@europarl.europa.eu |

29 April 2013

**Planned European Data Protection Regulation:**
**EPSM supports effective payment fraud prevention, incentives for pseudonymisation of payment data and one supervisory authority per data controller**

Dear Mr Albrecht,

the “European Association of Payment Service Providers for Merchants” is a specialized, internet-based association of payment service providers, which are typically non-banks. The 63 European members of the EPSM are typically involved at various stages of card and internet payment services.

As an association of payments specialists, we would like to draw your attention on the following topics, which are critical for fraud prevention activities and data security in particular.

## 1. General:

The payment industry has developed industry standards that aim at establishing secure and reliable networks. One of the objectives of these international standards, such as PCI and ISO 27001, has always been to provide the best security level possible, including the individuals’ rights. The ensuring of data protection is a key element of the industry in order to preserve the customers trust and confidence in electronic payments.

Although, establishing a sound security and data protection system throughout the whole processing chain has been a burdensome process for all entities, nonetheless it has been accepted globally. We believe that these security standards, which also cover the individual rights of the consumer, are consistent with the **European Central Bank's (ECB) Recommendations for the Security of Internet Payments**.

The ECB published its Recommendations for the Security of Internet Payments as well as draft Recommendations for Account Access Services on 31 January 2013[1]. One of the overarching principles is that payment providers are tasked to **perform risk analyses, fraud monitoring as well as logging and tracing of transactions in order to reduce fraud and to provide transaction data to law enforcement agencies**.

We believe that most of these recommendations are not only adequate but also necessary to mitigate fraudulent transactions to the benefit of the payer as such and to the functioning of electronic payment systems. Therefore, EPSM would very much appreciate **a coherent approach** from both the **European Central Bank** regarding the 'Security of Internet Payments' and the **European Parliament** regarding the 'General Data Protection Regulation'.

## 2. Anti Fraud

EPSM appreciates that **fraud** is clearly referenced in the definition of financial crime, that processing for anti fraud purposes is lawful, that there is no right to be forgotten for fraudsters, and that industry practises are acknowledged. Therefore, EPSM supports Amendments 803, 805, 862, 873, 874, 878, 880, 894, 1445, 1446, 1447, 1448, 1556, 1584, 1588 and 1590. In order not to contradict these principles, we believe that in Amendment 850 the possibility to 'monitor and detect fraud' should be included. As we believe that the requirements towards potential fraudsters should be limited, we are concerned about Amendments 100, 101, 102, 165, 876, 1545.

## 3. Incentivise Pseudonymisation

EPSM welcomes that **pseudonymisation** is incentivised by a number of amendments from LIBE committee members and therefore supports the Amendments 395, 415, 730, 734, 900, 1102, 1103, 1249, 1357, 1376, 1420 and 1585. In regard to Amendment 85, EPSM favours the deletion of the words '*is specific to one given context and which*', as this is likely to provide room for interpretation that could limit effective fraud prevention. As pseudonymisation should be incentivised, EPSM does not support Amendment 105.

## 4. One Supervisory Authority

EPSM supports the concept to have only **one supervisory authority per data controller**. Amendments 423, 424, 789, 790 as well as 2583 and 2592 are therefore supported. Amendment 277, requiring legally the involvement of other supervisory authorities before measures are adopted, is likely to minimise the effects of a 'one-stop-shop'.

Should you wish to receive further information, please do not hesitate to contact us.

Yours sincerely,

| | |
|---|---|
| Nicolas Adolph<br>Chairman of EPSM | Robert Komatz<br>Deputy Chairman of EPSM |

Enclosures

[1] Recommendations for The Security of Internet Payments and Recommendations for 'Payment Account Access' Services; both documents can be downloaded at the ECB website: http://www.ecb.int/press/pr/date/2013/html/pr130131_1.en.html

**Enclosure 1 - Amendments supported by EPSM**

| Amendment | Vote | Text of the Amendment |
|---|---|---|
| 395 | + | (23a) **This Regulation recognises that pseudonymisation is in the benefit of all data subjects as, by definition, personal data is altered so that it of itself cannot be attributed to a data subject without the use of additional data. By this, controllers should be encouraged to the practice of pseudonymising data.** |
| 415 | + | (25a) **This Regulation recognises that the pseudonymisation of data can help minimise the risks to privacy of data subjects. To the extent that a controller pseudonymises data, such processing should be considered justified as a legitimate interest of the controller.** |
| 423 | + | (27) **Where a controller or a processor has multiple establishments in the Union, including but not limited to cases where the controller or the processor is a group of undertakings,** the main establishment of a controller in the Union **for the purposes of this Regulation** should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore **not** determining criteria for a main establishment. **A group of undertakings may nominate a single main establishment** in the Union. |
| 424 | + | (28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. **A group of undertakings may nominate a single main establishment in the Union.** |
| 730 | + | (2a) **'pseudonymous data' means any personal data that has been collected, altered or otherwise processed so that it of itself cannot be attributed to a data subject without the use of additional data which is subject to separate and distinct technical and organisational controls to ensure such non attribution, or that such attribution would require a disproportionate amount of time, expense and effort;** |
| 734 | + | (2b) **'anonymous data' means any personal data that has been collected, altered or otherwise processed in such a way that it can no longer be attributed to a data subject; anonymous data shall not be considered personal data;** |
| 789 | + | (13) 'main establishment' means **both** as regards the controller **and as regards the processor**, the place **constituting** its **official seat** in the Union**, if that is the place** where the main decisions **of the institution, enterprise, or group are taken, or the latter place, if different**; |
| 790 | + | (13a) **'competent supervisory authority' means the supervisory authority which shall be solely competent for the supervision of a controller in accordance with Article 51(2), (3) and (4);** |
| 803 | + | (19a) **'financial crime' means criminal offences in connection with organised crime, racketeering, terrorism, terrorist financing, trafficking in human** |

|  |  |  |
|---|---|---|
|  |  | **beings, migrant smuggling, sexual exploitation, trafficking in narcotic drugs and psychotropic substances, illegal arms trafficking, trafficking in stolen goods, corruption, bribery, fraud, counterfeiting currency, counterfeiting and piracy of products, environmental offences, kidnapping, illegal restraint and hostage-taking, robbery, theft, smuggling, offences related to taxation, extortion, forgery, piracy, insider trading and market manipulation.** |
| 805 | + | (19a) **'financial crime' means criminal offences in connection with organised crime, racketeering, terrorism, terrorist financing, trafficking in human beings, migrant smuggling, sexual exploitation, trafficking in narcotic drugs and psychotropic substances, illegal arms trafficking, trafficking in stolen goods, corruption, bribery, fraud, counterfeiting currency, counterfeiting and piracy of products, environmental offences, kidnapping, illegal restraint and hostage-taking, robbery, theft, smuggling, offences related to taxation, extortion, forgery, piracy, insider trading and market manipulation.** |
| 862 | + | (c) processing is necessary for compliance with a legal obligation **or regulatory rule or industry code of practice, either domestically or internationally,** to which the controller is subject; |
| 873 | + | (f) processing is necessary for the purposes of the legitimate interests pursued by **the controller or by the third party or parties to whom the data are disclosed and of the legitimate expectations of the data subject based on his or her relationship with the** controller, **taking into account the** interests **or rights and freedoms of the controller to conduct a business as well as the** interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. |
| 874 | + | (f) processing is necessary for the purposes of the legitimate interests pursued by **the controller or by the third party or parties to whom the data are disclosed and the legitimate expectations of the data subject based on his or her relationship with the** controller, **taking into account the** interests **or rights and freedoms of the controller to conduct a business as well as** the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. |
| 878 | + | (f) processing is necessary for the purposes of the legitimate interests pursued by**, or on behalf of** a controller **or a processor, or by a third party or parties in whose interest the data is processed, including for the security of processing**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, **such as in the case of processing data pertaining to** a child. **The interest or fundamental rights and freedoms of the data subject** shall not **override** processing carried out by public authorities in the performance of their tasks. |
| 880 | + | (f) processing is necessary for the purposes of the legitimate interests pursued by a controller **or controllers or by a third party or parties to whom the data are disclosed**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. |
| 894 | + | (fb) **processing is necessary for fraud detection and prevention purposes according to applicable financial regulation or established industry, or professional body, codes of practice;** |
| 900 | + | (fd) **processing is necessary for the purpose of anonymisation or pseudonymisation of personal data;** |
| 1102 | + | If the data processed by a controller do not permit the controller to identify a natural |

| | | |
|---|---|---|
| | | person, **in particular when rendered anonymous or pseudonymous,** the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. |
| 1103 | + | If the data processed by a controller do not permit the controller **or a processor** to identify a natural person, **in particular when rendered anonymous or pseudononymous** the controller shall not be obliged to **process or** acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. |
| 1249 | + | (b) the data are not collected from the data subject and the provision of such information proves impossible **– for example because the data have been rendered pseudonymous –** or would involve a disproportionate effort; |
| 1357 | + | 3. The **data subject** shall **have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data which were provided by the data subject itself and that undergoing processing in an electronic and structured format which is commonly used and allows for further use by** the data subject**. This right shall not restrict rights of others as trade secrets or intellectual property rights**.<br>**This does not apply on the processing of anonymised and pseudonymised data, insofar as the data subject is not sufficiently identifiable on the basis of such data or identification would require the controller to undo the process of pseudonymisation**. |
| 1376 | + | **Paragraph 1 shall not apply to pseudonymous data.** |
| 1420 | + | 2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication. **Anonymised data, pseudonymised data and encrypted data are exempted, where compliance with this provision would require the controller to undo the process of anonymisation, pseudonymisation or encryption.** |
| 1445 | + | (da) **for the prevention or detection of criminal offences, in particular identity fraud against the data subject and financial crimes;** |
| 1446 | + | (ea) **for prevention or detection of fraud or other financial crime, confirming identity or determining creditworthiness.** |
| 1447 | + | (ea) **for purposes of the prevention and detection of fraud, and to the extent criminal data are processed, such processing is in accordance with Article 9(2) point j).** |
| 1448 | + | (ea) **for prevention or detection of fraud, confirming identity, and/or determining creditworthiness, or ability to pay.** |
| 1556 | + | 1b**. Is based on the legitimate interests** |
| 1584 | + | (ca) **is carried out in the purpose of monitoring and prevention of frauds;** |
| 1585 | + | (ca) **is limited to pseudonymised data. Such pseudonymised data must not be collated with data on the bearer of the pseudonym. Article19(3a) shall apply correspondingly.** |
| 1588 | + | (cd) **is necessary to pursue controller's legitimate interest in accordance with Article 6(1)(ja); or** |
| 1590 | + | (cf) **is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the profiles or data are disclosed, except** |

| | | |
|---|---|---|
| | | **where such interests are overridden by the fundamental rights and freedoms of the data subjects; or** |
| 2583 | + | 2. Where the **Regulation applies by virtue of Article 3(1), the competent supervisory authority will be the supervisory authority of the Member State or territory where the main establishment of** the controller or processor **subject to the Regulation** is established**. Disputes should be decided upon in accordance with the consistency mechanism set out in article 58, and this without prejudice to the other provisions of Chapter VII of this Regulation. This provision also apply for legal entities of a group of undertakings, where these undertakings are located in more than one Member State**. |
| 2592 | + | 2b. **Where the Regulation applies to several controllers and/ or processors with the same group of undertakings by virtue of Article 3(1) and (2), only one supervisory authority will be competent and it will be determined in accordance with Article 51(2).** |

**Enclosure 2:**
**Members of EPSM**

**Ordinary Members**

| | Main Activity | Country | City | Website |
|---|---|---|---|---|
| AGES | Network Operator | D | Langenfeld | www.ages.de |
| Anderson Zaks | Multi Channel Payment Provider | UK | Bracknell | www.andersonzaks.com |
| Atos Worldline (Banksys) | Acquirer | B | Brussels | www.banksys.com |
| B+S | Acquirer | D | Frankfurt/Main | www.bs-card-service.com |
| card complete | Acquirer | A | Wien | www.cardcomplete.com |
| CardProcess | Network Operator | D | Frankfurt/Main | www.cardprocess.de |
| cardtech | Network Operator | D | Köln | www.cardtech.de |
| CCV Allcash ecm | POS Payment Provider | D | Moers | www.ccv.eu |
| ConCardis | Acquirer | D | Eschborn | www.concardis.com |
| Deutsche Card Services | Acquirer | D | Köln | www.deutsche-card-services.de |
| DIBS | Internet Payment Provider | S | Stockholm | www.dibs.se |
| easycash | Network Operator + Acquirer | D | Ratingen | www.easycash.de |
| EDPS | Payment Service Provider | GR | Voula | www.edps.gr |
| Elavon | Acquirer | D | Frankfurt | www.elavon.com |
| EOS | Internet Payment Provider | D | Hamburg | www.eos-payment.com |
| Global Collect | Internet Payment Provider | NL | Hoofddorp | www.globalcollect.com |
| Hobex | Network Operator | A | Salzburg | www.hobex.at |
| ICP | Network Operator | D | Schwalbach | www.icp-companies.com |
| InterCard | Network Operator | D | Taufkirchen | www.intercard.de |
| LAVEGO | Network Operator | D | München | www.lavego.de |
| Lufthansa AirPlus | Acquirer | D | Neu-Isenburg | www.acceptance.de |
| montrada | Network Operator | D | Bad Vilbel | www.montrada.de |
| NETS | Network Operator | DK | Ballerup | www.nets.eu |
| Ogone | Internet Payment Provider | B | Brussels | www.ogone.com |
| PayLife | Acquirer | A | Wien | www.paylife.at |
| Paysafecard | Internet Payment Provider | A | Wien | www.paysafecard.com |
| Payvision | Payment Solution Provider | NL | Amsterdam | www.payvision.com |
| POSPartner | Payment Solution Provider | D | Königswinter | www.pospartner.de |
| Postbank P.O.S. Transact | Acquirer | D | Eschborn | www.postransact.de |
| SIX Payment Services | Acquiring, Processing Services – international Business EU wide | CH | Zürich | www.six-payment-services.com |
| SOFORT AG | Internet Payment Provider | D | Gauting | www.sofort.com |
| TeleCash | Payment Solution Provider | D | Bad Vilbel | www.telecash.de |

| | | | | |
|---|---|---|---|---|
| Transact | Network Operator | D | Martinsried/Planegg | www.transact-gmbh.de |
| VÖB-ZVD Processing | Network Operator | D | Köln | www.voeb-zvd.de |
| WEAT | Network Operator | D | Düsseldorf | www.weat.de |
| Wirecard CEE | Internet Payment Provider | A | Klagenfurt | www.wirecard.at |
| Worldpay | Internet Payment Provider | NL | Bunnik | www.worldpay.com |
| Yapital | Payment Provider | D | Hamburg | www.yapital.com |

**Extraordinary Members**

| | | | | |
|---|---|---|---|---|
| Acertigo | PCI Auditor | D | Stuttgart | www.acertigo.com |
| American Express | Payment Scheme | UK | Brighton | www.americanexpress.com |
| Atos Worldline | Acquiring Processor | D | Aachen | www.atosorigin.com |
| Cartes Bancaires "CB" | Payment Scheme | F | Paris | www.cartes-bancaires.com |
| CCV Deutschland | Terminal Manufacturer | D | Au i.d. Hallertau | www.ccv-deutschland.de |
| Clear2Pay | Service Provider | B | Zaventem | www.clear2pay.com |
| CUP | Payment Scheme | F | Paris | www.chinaunionpay.com |
| DAFÜR | Service Provider | D | Ober-Ramstadt | www.dafuer.com |
| Deutsche Telekom | Service Provider | D | Osnabrück | www.telekom.de |
| EQUENS | Payment Processor | NL | Utrecht | www.equens.com |
| EURO Kartensysteme | Service Provider | D | Frankfurt/Main | www.eurokartensysteme.de |
| FEXCO Merchant Services | Service Provider | IE | Kerry | www.fexcoms.com |
| Global Payments Europe | Payment Provider | CZ | Prague | www.globalpaymentsinc.com |
| HUTH Elektronik | Terminal Manufacturer | D | Troisdorf-Spich | www.huth-elektronik.de |
| Ingenico | Terminal Manufacturer | D | Berlin | www.ingenico.de |
| Lyra | Network Provider | F | Labege, Cedex | www.lyra-network.com |
| MasterCard Europe | Payment Scheme | B | Waterloo | www.mastercard.com |
| OmniPay | Acquiring Processor | IE | Dublin | www.omnipaygroup.com |
| payfair | Payment Scheme | CH | Zug | www.payfair.com |
| Scheidt & Bachmann | Terminal Manufacturer | D | Moenchengladbach | www.scheidt-bachmann.de |
| TNS | Service Provider | D | Neu-Isenburg | www.tnsi.com |
| Trustwave | Security Solutions | UK | London | www.trustwave.com |
| TSYS | Acquiring Processor | D | Frankfurt | www.tsys.com |
| VeriFone | Terminal Manufacturer | D | Bad Hersfeld | www.verifone.com |
| VISA EU | Payment Scheme | UK | London | www.visa.com |