



eBay is a registered organisation in the European Commission Register of Interest Representatives.

Name and address: eBay EU Liaison Office: 44 Avenue des Arts, 1040 Brussels, Belgium.

Registration number: 40386322300-77.

January 2011

eBay's submission to the European Commission's Consultation on the Communication 'A comprehensive approach on personal data protection in the European Union'

About eBay Inc.

Founded in 1995, eBay Inc. connects hundreds of millions of people around the world every day, empowering them to explore new opportunities and innovate together. eBay Inc. does this by providing the Internet platforms of choice for global commerce and payments. Since its inception, eBay Inc. has expanded to include some of the strongest brands in the world, including eBay, PayPal, Marktplaats, StubHub, Shopping.com, and others. eBay Inc. is headquartered in San Jose, California.

Our contribution to this consultation focuses on our two major services based in the European Union, that is eBay Marketplaces and PayPal. eBay aims to create, maintain and expand the functionality, safety, ease-of-use and reliability of its online commerce platforms while, at the same time, supporting the growth and success of its community of users. PayPal allows consumers to pay and get paid online across different locations, currencies, and languages. Having built a single global payments engine that has some of the best risk and fraud detection capabilities in the payments industry, PayPal continues to be one of the leading ways to pay online.



Contents

Introduction	3
1. Definitions	5
A. Definition of personal data	5
2. Principles	6
A. Applicable law: the principle of country of origin	6
B. The ‘Right to be forgotten’	8
3. Business Cases	8
A. Mergers and Acquisitions	8
B. Intra-group data sharing	9
C. Fraud Detection and Anti-Money Laundering	9
4. International consistency	10
Conclusion	11



Introduction

eBay Inc welcomes the European Commission's consultation on the Communication 'A comprehensive approach on personal data protection in the European Union'. eBay has always engaged in the dialogue that the Commission launched back in 2009 as regards data protection¹, sharing its broad views on the legal framework enshrined in Directive 95/46/EC. As the consultation process evolves, we would like to make some more specific comments on the impact that the revision may have on online businesses such as ours. As leading e-commerce platforms and online payment services operating in both EU and non-EU countries, we believe our first-hand experience and top-level compliance when dealing with personal data are to be taken into account in light of the current revision of the Directive.

eBay Inc. is a publically traded entity whose primary stock market listing is the NASDAQ exchange in the United States of America. The firm has a market presence in over 25 countries globally. In the European Union our two major Services' EU headquarters (that is, eBay and PayPal) are located in Luxembourg. eBay Europe S.à.r.l., a Luxembourg company, is the legal entity that EU-based users contract with to benefit from eBay services. PayPal's European headquarters, PayPal Europe S.à.r.l. & Cie, S.C.A., is a Luxembourg bank licensed by the *Commission de surveillance du secteur financier*, and the legal entity that EU-based users contract with to receive payment services.

Because all EU-based users of eBay.com contract exclusively with eBay Europe S.à.r.l, this Luxembourg entity is the designated data Controller for all EU eBay.com user data, such as eBay.de user data. eBay Europe is the data Controller in *fact*, as well as *law*. It is responsible for the governance of service provision, determining the purpose and means of personal data management - meeting the statutory definition of a Controller. This framework has been officially approved by 14 EU Data Protection Authorities through eBay's successful Binding Corporate Rules application, whereby eBay's lead Data Protection Authority is the *Commission Nationale pour la Protection des Données* (CNPD) for user data².

eBay's privacy function operates an internal control system that aligns current and *ex ante* legal requirements to our operating processes. This alignment occurs through a variety of consulting, advocacy and executive oversight mechanisms.

¹ See eBay's response to Consultation on the legal framework for the fundamental right to protection of personal data (December 2009): http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/eBay_en.pdf and Targeted consultation and meeting dating back in July 2010.

² See press release: <http://www.cnpd.public.lu/fr/actualites/international/2009/11/eBay/communiqu-eBay.pdf>



Individuals choose to share personal information about themselves, in order to build trust with each other, in our platforms. Protecting personal data is therefore fundamental to our marketplaces ecosystem, because increased protection encourages broader data exchange, a more efficient market and, as such, higher transaction volume. The data managed by businesses about the consumer form the very basis of a long-term customer relationship and our businesses' competitive advantage. For instance, our payments system PayPal allows consumers to pay for transactions without exposing their financial information. As such, we believe PayPal to be the most privacy protective payment mechanism commercially available today, demonstrating that the principle of 'privacy by design' has economic value, as a competitive differentiator.

Our contribution aims at showing that an innovation-driven, technology-neutral and flexible regulatory approach is not incompatible with a high degree of personal data protection. On the contrary, eBay Inc. believes that an objective-orientated regulatory framework will ensure that both ambitions of the protection of fundamental rights and the achievement of the internal market are completed, paving the way for a competitively enhanced digital Europe.

1. Definitions

In this section, eBay wishes to comment in particular on the current debates around the definition of personal data.

A. Definition of personal data

In its Communication, the Commission recognizes that the non specific definition of personal data contained in the current Directive is a deliberate approach which has the benefit of flexibility and applicability. However, the Communication alludes to ‘grey areas’ that would require additional measures under Union law.

eBay wishes to highlight that there are no ‘grey areas’ as such but rather data that are processed in a specific context, which determines whether they are to be considered as personal, i.e. related to an ‘identified or identifiable person, either directly or indirectly’, or not. Geolocation data is a good example to illustrate that notion of context.

Geolocation as regulated by Directive 2009/136/EC is currently being transposed by Member States into national law. The Directive defines “location data” as “*any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*”. Location data relating to a subscriber or user of a public electronic communications network may only be processed where:

- the subscriber or user cannot be identified from that data; or
- where it is necessary to provide a value added service with the consent of the relevant user or subscriber.

Credit card companies have used essentially real-time location data for many years as part of verification and fraud prevention activities. Subsequently, geolocation data transmitted from a mobile device can inform a data Controllers internal control system, and as such represents legitimate processing of the Controller to protect its interests and those of its users.

Geolocation data can also add value to advertising processes that an increasing number of generational groups demand. Informed choice is the fundamental concept with which users are empowered to opt-out of geolocationally targeted advertising.

eBay believes it is important for regulation to support appropriate use of this data outside of network infrastructure as this data has important uses from fraud prevention to supporting advertising that consumers choose.



Similarly, IP addresses in many cases are simply not identifiable to an individual in a proportionate sense. Subsequently, it is for the data Controller to determine the safeguards provided on a case by case basis.

Flexibility, therefore, as well as technology neutrality, are important virtues to be applauded in 95/46/EC, as they enable data Controllers to provide protections to data subjects in a manner proportionate to the risks they actually face. Again, an objective-orientated approach to the definition of personal / sensitive data is the best way to guarantee the effectiveness of the upcoming regulatory framework.

2. Principles

eBay Inc. provides here its views on two important aspect of the Communication, which are the principle of country of origin as applicable data protection law and the so-called 'right to be forgotten'.

A. **Applicable law: the principle of country of origin**

In the Communication, the Commission states that it will examine how to revise and clarify the existing provisions on applicable law, *"in order to improve legal certainty, clarify Member States' responsibility for applying data protection rules and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller"*.

The Communication could be interpreted to say that the Commission considers abandoning the current "country of origin" principle as it related to data protection. Any changes to this principle would lead to severe negative consequences for companies operating efficiently cross-border.

The current principle of country of origin, i.e. the country where the data Controller is established, as applicable national law has been fundamental in supporting the internal market objective of the Directive. It sets the conditions for businesses to be established in one member state and service Union-wide, without facing an unnecessary compliance burden of duplicated requirements – with eventually no improvement in protections afforded to data subjects. eBay is currently active in 14 countries in the EU and rely for its users and business partners on one single point of contact which is the Luxembourg DPA. Moving to country of residence principle would mean unnecessarily duplicating efforts for both companies and DPAs. Therefore eBay is convinced that the current regime is actually the best framework to provide the exact same degree of protection for all eBay users, regardless of where they are based in Europe. Continuity of provisions here appears important.

More generally, some organisation designs have been informed by centralising data protection responsibilities into one jurisdiction. Centralising user data control under one DPA jurisdiction



provides the opportunity for consistency and standardised process design in control architecture, enabling user privacy rights to be experienced at a consistently high standard across the EU, and indeed globally in the case of our organization.

To the extent that DPAs collaborate today through the Article 29 Working Party and Article 31 Committee, we support broader collaboration and sharing of responsibilities between DPAs. Passporting in the financial services sector, where certain financial services can be carried out by a firm established in one country in the internal market and delivered into other countries in the internal market, is a good example of regulatory change supporting business growth. PayPal is a unique example of what can be achieved by a bank that has made privacy by design a central theme in its commercialization strategy, serving the entire EU marketplace for a single banking license / data Controller in Luxembourg.

Greater and more formal collaboration between DPAs, reflecting the spirit of the internal market, will go a long way to support and extend the sense of recourse citizens can achieve in enforcing their rights. eBay would like to highlight that as a Luxembourg data Controller, we have engaged in consultation with various DPAs, encouraging them to bring issues to our attention regardless of jurisdiction. We have voluntarily agreed to respond to these issues directly with the DPA who raised the issue, informing our competent Luxembourg DPA, of all such matters. We do this not because we are required to, but because it's the right thing to do for our users. For similar reasons, we have successfully adopted Binding Corporate Rules, to inform our global standard on data protection.

Finally, eBay believes that one of the most successful aspects of 95/46/EC has been its division between data Controller and data Processors. Although in practice such divisions are often complicated, this is necessarily so to reflect what is often a complex reality, and we applaud the Article 29 Working Party continued efforts to advise on this matter.

We feel that obligations pursuant upon data Processors should not necessarily be increased, as this may tend to blur the distinction of accountability potentially to the detriment of the data subject. Rather, any change in requirements should be pursuant upon data Controllers as the entity which determines processing in law and in fact. As such, accountabilities are concentrated, not diluted and this will in practical terms tend to strengthen protections to data subjects.

To conclude on this section, eBay considers the Directive and the related mechanisms (including the necessary recourses) are already in place to enable consistent protections across the EU. The way to ensure a consistent level of protection and even to improve it is not to put the current legislation into question but rather to evolve it through the work of the Article 29 Working Party and through the Commission's work in ensuring the Directives are correctly implemented.

B. The ‘Right to be forgotten’

After intense debates at national and European level, the Commission included the so-called ‘right to be forgotten’ into the Communication. It is defined as the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. First of all, eBay wishes to highlight that the corresponding legislation already exist in Directive 95/46/EC: the obligation to keep data only as long as necessary for the purposes for which these have been collected, coupled with the right in some contexts to have data deleted and the right to withdraw consent are components of the “right to be forgotten”.

As such, some Controllers have many legitimate reasons ‘not to forget’ users’ personal data including for fraud detection and Anti-Money Laundering purposes. Similarly, many regulatory and best practice requirements compel preservation of records. Finally, Controllers may keep data of inactive users, who frequently re-engage with service providers.

Nevertheless, at some point, it indeed makes no sense to retain data from any perspective, and this follows from associating retention with the context of purpose and use of legitimately processed personal data.

3. Business Cases

In this section, we aim to provide some ‘real-life examples’ of situations where personal data are at stake in the daily activities of (online) businesses. We focus on mergers and acquisitions, intra-group data sharing and fraud detection and anti-money laundering.

A. Mergers and Acquisitions

An important aspect of the free flow of personal data within the Internal Market is data shared in case of mergers and acquisitions of private legal entities.

In the course of its business, companies like eBay Inc. may consider the acquisition of other organizations. In doing so, those acquired entities are transitioned to our technology and governance framework, and subsequently benefit from our long standing and evidenceable commitment to privacy.

The planning and execution process of an acquisition for eBay Inc. contains privacy due diligence components, and to the extent that we detect that the overall governance of personal data in an acquisition target has been less effectual than the treatment it would have received from eBay, we would find grounds for lowering the acquisition price due to investment necessary to bring that organisations’ privacy levels up to eBay standards.



For a firm such as eBay who has made a verified and sustained long term investment in privacy, a mandated opt-in approach for a change in Controllershship would create instability and cost. Shareholders could be penalised by the acquisition of overvalued organisations, and some businesses valuations may be downgraded because they themselves become less attractive takeover targets.

More fundamentally, from the perspective of a data Controller who has been granted Binding Corporate Rules approval, our general approach to informed consent provides a bedrock from which we inform users in an acquired entity of their new Controller, and provides the basis for them to opt-out of this relationship, if they so choose.

Therefore we encourage the European Commission to maintain this regime of requirements around transferability of obligations and rights, thus promoting users choice and continuity in investment planning and financial accounting processes.

B. Intra-group data sharing

We live today in the age of globally integrated businesses and intra-group data sharing is a fundamental dimension of this environment. In that sense, Binding Corporate Rules have been significant gains in streamlining the process of intra-group data sharing.

eBay believes data exchange within a corporate group that achieves a demonstrably high standard of privacy compliance should be supported. Individuals who contract with different data Controllers who are part of the same corporate group generally do so under privacy policies which disclose that shared systems, processes and infrastructure make some legitimate degree of data sharing inevitable. To the extent that data sharing in this context were to become more constrained, significant costs would be incurred by Controllers, which would not support the enhancement of protections afforded to data subjects.

The benefit for data subjects who interact with eBay companies is that privacy responsibilities as set out in our Binding Corporate Rules are discharged under a holding company mandate, so there is consistency of application, in law and in fact, across all Business Units.

C. Fraud Detection and Anti-Money Laundering

When a data Controller is faced with a significant risk of fraud, it is within its rights to process personal data in order to protect itself and users of the service in question. Similarly, regulatory requirements such as Anti-Money Laundering legislation compel Controllers to process personal data in order to comply with statutory obligations. As such, continuity in these provisions appears important.

Anti-Money Laundering and fraud issues often do not know national boundaries and can require transfers outside of the EU on a regular basis. Thus clarity and recognition of this fact would be



welcome. Greater collaboration between DPAs and other international regulatory agencies, for instance financial service regulators outside the EU, would also provide useful for many data Controllers.

Disparate entities located in third countries have mandatory obligations to comply with local legal requirements that sometimes require disclosure of personal data to support Anti-Money Laundering obligations. This can pose complexities for data Controllers and as such more prescriptive guidance on reconciling differing legal requirements would provide useful.

Finally, we would like to address the aspect of law enforcement and government requests for data. eBay and PayPal as Luxembourg data Controllers receive a significant volume of disclosure requests from non Luxembourg law enforcement and governmental bodies. In processing these requests, we are informed by both legal obligations compelling disclosure, and a balance of interest test where the privacy protections of our users are duly considered. In this situation, limiting the statutory obligations on Controllers to disclose user data to more specific and targeted requests would likely reduce the volume of 'false positives' by the requestor, and provide greater protection of privacy to our users. We think this also falls into the requirement for more international consistency (see below).

4. International consistency

The extra-territorial provisions of European data protection make international and intergovernmental collaboration important and are to be supported.

Multinational corporations routinely face a complex set of sometimes contradictory regulatory requirements. To the extent that these emanate from the extra-territorial provisions of 95/46/EC, then international and intergovernmental collaboration is to be welcomed. A good example of this has been the recent Article 29 Working Party paper on pre-trial discovery, and the subsequent discourse at the Sedona conference. Finding robust legal solutions to support processing of personal data as it relates to third country litigation, particularly in civil coded legal systems is welcomed by eBay.

On our part, we have raised data protection points in various consultation processes with regulatory bodies outside the EU, such as the FINcen consultation on cross-border electronic fund transmission.

Inside the European Union itself, there is sometimes a lack of consistency and collaboration between Member States, particularly in the case of governmental requests for third party information, placing a significant burden on businesses and potentially compromising consumer protections. While we fully recognize our covenant to collaborate with various governmental



bodies' access requests for data, we are also fully accountable to protect the privacy of our users.

eBay faces thousands of requests from various governmental agencies throughout the EU for personal customer information. These agencies, such as customs, tax and law enforcement authorities, typically will not follow the appropriate national procedures and instead opt for their own *ad hoc* procedures that put eBay in double jeopardy. Our subsidiaries that process information may face a broad gambit of penalties for not complying with a local order and likewise our Luxembourg data Controller may be penalised under data protection laws for permitting a subsidiary from another EU Member State to hand over the personal information of a user.

To be clear, eBay does lawfully process thousands of individualised requests for personal customer information where the requests are directed at the Luxembourg data controller, are specific to an identifiable customer, and meet the requirements of Luxembourg data protection law. eBay also provides tools to improve the speed and efficiency of our cooperation with law enforcement authorities including means through which authorized law enforcement staff can submit and receive standard data requests electronically.

eBay urges the Commission to review the cooperation protocols between Member States and provide clearer guidelines on how an agency may validly request personal customer information from and organisation, their subsidiaries and processors.

From our perspective as a Luxembourg data Controller, subject in essence exclusively to Luxembourg data protection law for our EU eBay and PayPal users, we have adopted an open and transparent position with our competent regulators on extra territorial regulatory challenges we face. In so doing the knowledge we have gained has informed our internal due process and to this extent we welcome opportunities to share our leanings, given our belief in open consultation.

Conclusion

eBay Inc. looks forward to working with the European Commission to share our experience and expertise when it comes to the protection of personal data in the European Union and abroad. We would be happy to discuss these points and the broader revision of Directive 95/46/EC into more details once the written consultation period closes. To that end, please do not hesitate to contact us.



For further information, please contact:

Steve Kenny, Head of EU Privacy, eBay Inc.

T: +35 (0)2 621 309 917

E : stkenny@ebay.com

Maija Haas, Senior Manager EU Public Affairs, PayPal

T: +32 (0)2 788 97 41

E : mhaas@paypal.com

Claire Vasile, Manager EU Public Affairs, eBay EU Liaison Office

T: +32 (0)2 788 97 16

E: cvasile@ebay.com

Further information on eBay's EU Government Relations activities is available from our website:

www.ebay.eu/governmentrelations