49.

EUROPEAN ASSOCIATION OF CO-OPERATIVE BANKS
The Co-operative Difference : Sustainability, Proximity, Governance

Brussels, 31 January 2017

EACB's views on the Article 29 Working Party Guidelines on the right to data portability and on Data Protection Officers

The **European Association of Co-operative Banks** (EACB) is the voice of the co-operative banks in Europe. It represents, promotes and defends the common interests of its 28 member institutions and of co-operative banks in general. Co-operative banks form decentralised networks which are subject to banking as well as co-operative legislation. Democracy, transparency and proximity are the three key characteristics of the co-operative banks' business model. With 4,050 locally operating banks and 58,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 210 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 79 million members and 749,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the opportunity to provide the Article 29 Working Party (WP29) with its comments on the draft Guidelines adopted in December 2016. The EACB's main concerns relate to the Guidelines on the Right to Data Portability, and only a few to the Guidelines on Data Protection Officers (DPOs).

Comments on the Guidelines on the Right to Data Portability

General Comments

Co-operative banks welcomes the WP29's guidance to data controllers in clarifying the meaning and application of data portability, which is a new right that provides consumers with greater control over their personal data, notably in how it facilitates switching between different service providers.

As the WP29 righty states, switching is one of the main benefits of data portability, and this new right can therefore prove useful in many instances where switching providers is currently difficult due to obstacles to the free flow of personal data. However, we note that banking is already a heavily regulated sector in this respect, with broad consumer protection rules that offer costumers the ability to easily switch from one service provider to another. Data portability in the banking sector, therefore, needs to be approached with caution and interpreted strictly in light of existing legislation.

When interpreting Article 20 of the GDPR, it should be kept in mind that the right to data portability was created with major internet companies in mind. The leading idea was to promote consumer switching by preventing so-called lock-in-effects. Lock-in becomes a concern when companies achieve large market dominance or become an essential facility (e.g. Facebook) and then impede competition. In the case of payment institutions, it should be generally noted that the prevention of lock-in effects has been specifically addressed by Directive 2014/92/EU of the European Parliament and of the Council on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (Payment Accounts Directive (PAD)). Indeed, one of the aims of the PAD is to facilitate switching of payment accounts by establishing minimum standards and to make switching more attractive to consumers and promote competition.

Given that both the right to data portability and the PAD have as common aim to facilitate switching from one service provider to another, thus enhancing competition between services as clearly stated in the Guidelines, we put forward that when applied to banks the right to data portability should stay within the confines established by the PAD and not include data that does not affect consumers' ability to switch providers.

Specific concerns

1. Data Portability

The EACB welcomes the WP29's clarification that '*any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.*' However, we are concerned about the wide interpretation given by the WP29 to Article 20(1) when it comes to data 'provided by' the data subject. The draft Guidelines state that data generated by, collected from the activities of, or resulting from the observation

of the activities of users is covered by the right to data portability. We believe this is a broad interpretation of the Article 20 provisions that goes unnecessarily beyond the end goal of Article 20, which attempts to find a balance between the data subject's interest in obtaining his or her data for the purpose of switching to an alternative provider and the data controller's obligations.

Indeed, given that the main objective of data portability is to facilitate switching, it should be kept in mind that switching is already provided by banks and regulated in Europe. For customers to switch their account (or even a securities account) to another bank, only information about the current status of the account (balance, standing instructions, securities positions, etc.) is needed, but not all the data ever provided by the client, that is, historical data that bears no effect on the current account balance. Therefore, data portability should focus on 'all data provided by the client, which is relevant for switching to an other provider for a given service'.

2. Need for the Guidelines to stay within the boundaries of what the GDPR has stipulated

Co-operative banks believe that some of the recommendations suggested by the Guidelines go well beyond the requirements set forth in the GDPR.
In particular, we note that the draft Guidelines suggest that *'data controllers should offer different implementations of the right to data portability. For instance, they should offer a direct download opportunity for the data subject but should also allow data subjects to directly transmit the data to another data controller. This could be implemented by making an API available. Data subjects may also wish to use a personal data store or a trusted third party, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required, so data can be transferred easily from one controller to another.'* Furthermore, the draft Guidelines state that *'all data controllers (both the "sending" and the "receiving" parties) should implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data.'*

We believe that no technical requirements should be set for the way in which the portability would have to be supported and can see no legal basis for such requirements in the GDPR. In addition, we would like to note that, as regards technical requirements, clear rules are already laid down under the Payment Services Directive 2 (PSD 2), which stipulates that banks shall make it possible for third-party providers to rely on the authentication procedures provided by banks, allowing third-party providers to have access to clients' payment accounts and customer data information via the banks' infrastructure. Any divergence from these provisions should be avoided.

Another area where we believe the Guidelines go beyond the boundaries of the GDPR is where they state that *'data controllers [should] always include information about the right to data portability before any account closure.'* The GDPR requires to inform the data subject about the right to data portability at the moment the data is obtained (Art. 13.2(b)), no where does it mention that this would have to be communicated again at the point of account closure.

3. Controllership

The draft Guidelines specify that *'[d]ata controllers answering data portability requests, under the conditions set forth in Article 20, are not responsible for the processing handled by the data subject or by another company receiving personal data.'* They continue saying that *'At the same time, a receiving data controller is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing. [...] in the case a data subject request transmission of details of his or her bank transactions to a service that assists in*

managing his or her budget, the new data controller does not need to retain all the details of the transactions once they have been labelled.'

Firstly, we'd like to ask the WP29 to better clarify what is meant by 'label'. In any event, we'd like to stress that, as far as banking institutions are concerned, the very same objectives and concepts put forward by the example in the draft Guidelines already form the basis of the Payment Services Directive 2 (PSD2).

Precisely as in the example provided by the WP29 in the draft Guidelines, the PSD2 was conceived in light of the new services provided by third-party providers, e.g. account information services allowing consumers to collect and consolidate information on their different bank accounts in a single place, allowing for consumers to have an overview of and analyse their spending patterns and financial needs. The PSD2 aims to remove barriers preventing such service providers from entering the market of payments and offering their solutions on a large scale and in different Member States, thus creating more competition and innovation.

The PSD2 stipulates that account information service providers, acting as new data controllers under data protection rules, should only access from banks the information explicitly consented by the payer and only to the extent they are necessary for the service provided to the payer, hence abiding by the principle of data minimisation.

Co-operative banks believe that in relation to banking data, given the considerable overlap in objectives between the right to data portability and the PSD2, and given the specific tools already available through the latter, the Guidelines should refrain from interpreting the right to data portability in a way that diverges from the PSD2. On the contrary, we urge WP29 to explicitly mention the PSD2 in its Guidelines and to recognise that the PSD2 provisions act a sectorial implementation of the right to data portability.

4. Personal data concerning other data subjects

We are concerned by language contained in the draft Guidelines suggesting that providers should actively facilitate switching not only in relation to the customer who is exercising his or her right to data portability on his or her own request, but also in relation to customers who have not made any request to port their data. In particular, the draft Guidelines state that providers '*should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. because they as well want to move their data to some other data controller.*' We believe this consent mechanism is not only impractical, firstly because banks don't have relationships with all the subjects involved in their customers' transactions, but would also place providers in the awkward position of having to actively promote competitors.

Additionally, we respectfully disagree with the draft Guidelines' assertion (p. 9) that '*the rights and freedoms of the third parties are unlikely to be adversely affected in the ... bank account history transmission, if their data are used for the same purpose in each processing, i.e. ... as a history of one of the data subject's bank account.*' Whether they are customers or not, the relationship of a private person to a banking institution relies mainly on factors of trust and integrity especially in dealing with provided data. Relying solely on the goodwill of the receiving controller to not use the transmitted third party data for its own purposes ignores that the wording of Article 20(4) of the GDPR does not narrow this obligation to one party, but perpetuates a general principle that puts an obligation on all controllers involved.

- The DPO is invited to participate regularly in meetings of senior and middle management.
- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.'

We believe that the procedure suggested by the WP29 is too complex and overly burdensome to the extent that it aims to generalise the DPO's involvement in companies' daily operations, i.e., participation in senior and middle management meetings, beyond what is required by the DPO's task. We believe DPOs should be involved promptly but only for decisions that have a clear data protection impact.

Finally, it might be helpful if the Guidelines could specify that a DPO's function may also be carried out by a data controller's compliance department, considering that this function also operates independently in banks.

- Conflict of interest

Co-operative banks believe that banks should be allowed to define the DPO's position freely depending on their existing organisation. In particular, attention must be paid to the interests and practical needs of small and medium-sized enterprises concerning the position of the DPO.

Notably, it might be more efficient for SMEs to assign the task of DPO to its 'statutory agents' (e.g. money laundering officers, compliance officers). However, this seems to run against footnote 34 of the draft Guidelines (page 16), which states: *'As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.'* We believe this reading will unnecessarily create additional costs and complexity for smaller organisations such as co-operative banks.

- **Tasks of the DPO**

- The DPO's role in a data protection impact assessment

We would recommend that the wording *'If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account'* in the Guidelines should be replaced by *'If the controller disagrees with the advice provided by the DPO, the DPIA documentation should* ***describe how the data controller will implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR'.***

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

[redacted] Head of Department Retail Banking, Payments, Financial

[redacted] Adviser Consumer and Retail Banking

5. Cost to data controller to satisfy data portability requests

Acknowledging that Art. 12 of the GDPR prohibits the data controller from charging a fee for the provision of personal data, unless the data controller can demonstrate that the requests from a data subject are manifestly unfounded or excessive, *'in particular because of their repetitive character'*, co-operative banks would like to receive more clarity on what might constitute excessive or repetitive requests that can be refused or justify a fee.

Furthermore, the draft Guidelines claim that automated processing by information society services – therefore including online banking – are *'very unlikely'* to be caused excessive burden by multiple data portability requests. We believe that such an assumption is unfounded and lacks any observation with regard to the actual implementation of the right to data portability. We submit that co-operative banks are, quite on the contrary, likely to incur considerable costs linked to the complex technical work that will be necessary in order to comply with the requirements of the new right of data portability.

Comments on the Guidelines on Data Protection Officers (DPOs)

Co-operative banks welcome the Guidelines on the Data Protection Officers (DPOs).

For many of our members, the requirements reported by the WP29 largely correspond to the existing requirements under their national laws for the activities of an operational data protection officer.

However, we would like to call the WP29's attention on some aspects that should be taken into consideration when formulating the requirements:

- **'Easily accessible from each establishment'**

Article 37(2) of the GDPR allows a group of undertakings to designate a single DPO provided that he or she is *'easily accessible from each establishment'*. We would welcome it if the Guidelines could clarify that this accessibility requirement should allow sufficient organisational flexibility, for instance by also using video conferencing or other electronic means.

- **DPO on the basis of a service contract**

The draft Guidelines clarify that *'the function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation'* (page 12).

While we generally agree with the recommendations contained in the Guidelines, we'd like to note that the mention of the external organisation's lead contact in the service contract might in practice prove beyond the point to the extent that such organisation should have the flexibility to reassign tasks internally, and hence also the designated lead, so long as the GDPR provisions are abided by. We therefore believe that the identification of the lead person 'in charge' should not be part of the contract.

- **Position of the DPO**

  - *Involvement of the DPO in all issues relating to the protection of personal data*

The draft Guidelines specify that the DPO is informed and consulted *'about all the projects dealing with data processing activities within the organisation. 'Consequently, the organisation should ensure that:*