GDPR how it affects EU BIN sponsors with non EU processors

Written by: Simon Hinks and David Parker

January 2018

The General Data Protection Regulation (GDPR) is a new version of EU Data Protection law to replace the 1995 Data Protection Directive, and in turn our Data Protection Act 1998. Despite the Brexit vote, the UK Government is committed to adopting the GDPR, and a Data Protection Bill is currently making its way through Parliament to give effect to some of GDPR's provisions.

Key to remember is that under the new regulations the end user always remains the owner of their data. The EU GDPR has within it eight core principles or rights focusing on the accountability associated with looking after an individual's personal details. These new rights include such things as automated decision making including the profiling process plus the right to restrict processing of personal data. The ICO is setting a level playing field for all organisations who want to work or sell products and services to citizens into and out of the EU.

In the world of Emoney there are normally four main parties to be considered in the delivery of a prepaid or Emoney Debit product:

1. Issuer
2. Processor
3. Programme Manager
4. Consumer

This white paper briefly touches on what happens if the processor and thus the data processor is outside the EU, when other parties are inside. Of course this is only one option on how Polymath Consulting can help Issuers, Processors and Programme Managers work through what the implications are if any one or more of the four parties sit outside the EU or even if they all sit inside the EU.

By the 25th May this year the GDPR regulations become enforceable by the ICO and one of the biggest changes is the implication of personal data being transferred outside of the EU. This can only take place under certain compliance conditions. These conditions are to ensure adequate safeguards are in place and can only take place where the

"*Commission has decided a third country, territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.*"

Article 28(1) specifically spells out for the processors that:
Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

So simply put, data controllers, i.e. customers of data processors, must choose data processors that comply with the GDPR. A data processor is anyone who processes personal data on behalf of the data controller.

The definition of a data controller, is stated in the Regulation's Article 4 (7) as:
'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

So any data controller needs to check to see if your processor is from a country already recognised by the ICO with adequate levels of security in their regulations and look for written evidence that compliance with the EU GDPR is the frame work the processor works within. Choose carefully who your processor is as BIN sponsors and Programme Managers within the EU as data controllers are just as liable for data breaches as the processor.

Role	Role in Relationship	Data Held
Issuer	Issuer of cards, legal contract between issuer and Program Manager (PM) to issue the cards as a scheme member	KYC info, full name and address
Programme Manager	Contacts processors and Bank so they pull everything together, may manage a wallet that feeds the card. PM holds the contracted relationship with the corporate client.	Sometimes KYC info, transactions, may or may not have PAN
Processor	Holds all data relating to card and transactions	KYC info, transactions, PAN

Issuer	Processor	Prog Mgr	Consumer	GDPR Impact
Inside EU	Outside EU	Inside EU	Inside EU	Medium to high dependent upon whether the processor sits within an ICO recognised country for compliant safety standards in-line with GDPR

Terms

GDPR	General Data Protection Regulation
ICO	Information Commissioners Office – the Regulator
BCR	Binding Corporate Rules
Personal Data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

How can Polymath Consulting Support You

Polymath Consulting is all about hands on practical support with senior consultants who know and understand the issues you face. With an unparalleled reputation in EMoney we believe we have the expertise to support you.

Typically our work takes a two stage approach:

1. **Light Touch Assessment**

   Taking just a few days we will review where you are today, what your plans are and what the issues you will face in being ready for GDPR. In effect a gap analysis. Whether already with plans in progress where we just sense check them, or as a starting point we can either confirm the current plans or create a road map to enable you to ensure you are fully complaint.

2. **Accelerated Preparation and On-Going Support**

   With a team of experts and experience we can support you both in accelerating your existing plans or in helping create them. In addition to just planning though with the right resource we can assist with all the aspects around people, platforms and places – as required by Article 30 in the GDPR