WHAT THE GDPR* MEANS FOR PAYMENTS?

ADOPTED 14 APRIL 2016

APPLIES 25 MAY 2018

European Payments Council

**Genaral Data Protection Regulation*

The GDPR significantly revises and harmonises how consumers' personal data shall be protected in the European Union. When it comes to data privacy, payments might be one of the most sensitive areas for consumers.

PAYMENTS: WHAT WILL GDPR MAINLY CHANGE FOR PSPs

Following the provisions of the GDPR, PSPs can process personal data:

With the data subject's consent

OR

Because processing is required:

- To ensure the performance of a contract
- To comply with a legal obligation
- To safeguard a data subject's vital interests
- For the purposes of legitimate interests*

**Except where such interests are overridden by the interests, rights or freedoms of the individual*

WHAT IS NEW FOR PSPs ?

- Wider territorial scope
- Increased accountability requirements
- Processing of personal data strengthened & rights of individuals widened
- Fines for non compliance up to 20,000,000 euros or 4% of worldwide group turnover

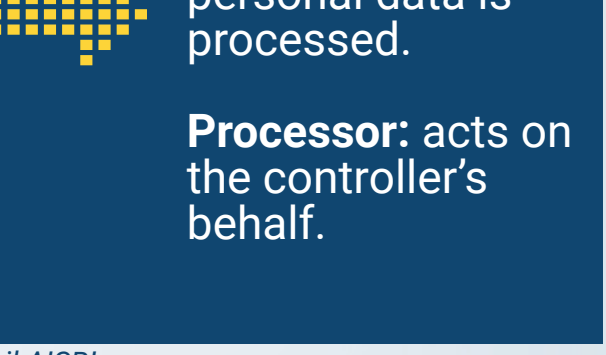
ROADMAP FOR PSPs TO BE GDPR COMPLIANT

PSPs must ensure that the personal data they process are:

- Processed legally and appropriately and with a clear view of how the information will be used;
- Collected for specified, explicit and legitimate purposes;
- Relevant and limited to the respective purposes;
- Accurate and kept up to date;
- Only processed if the data are kept appropriately secure.
- Retained for no longer than is necessary for the relevant purposes;

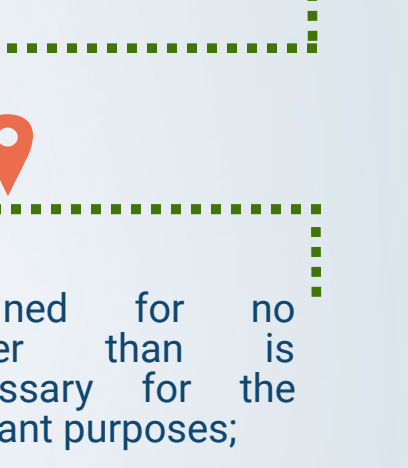
4 POINT CHECKLIST FOR PSPs

- *Review all data processing activities and keep verifiable records of these activities;*
- *Ensure that you have implemented appropriate technical and organisational measures to adequately protect the security of the personal data of your clients ('data protection by design and by default');*
- *Ensure compliance with the 'accountability principle' and cooperate with the relevant supervisory authority where appropriate;*
- *Ensure that you have appropriate processes and templates in place for identifying, reviewing and promptly reporting data breaches to the relevant supervisory authority.*



GDPR vs PSD2

The PSD2 notion of 'sensitive payment data' (i.e. data, including personalised security credentials, which can be used to carry out fraud) is not to be confused with the special categories of personal data under GDPR.



PSD2 stipulates that PSPs shall only access/process/retain data necessary for the provision of the services, with the explicit consent of the user. Whereas under the GDPR, consent is just one of the possible grounds for processing personal data.

Third party payment service providers (TPPs) and ASPSPs alike should not overlook the GDPR's strict purpose limitation/data minimisation principles when considering to further use personal data obtained in accordance with the requirements of PSD2.

PSPs should assess on a case by case which provisions of PSD2 and GDPR apply to a concrete situation. In doing so, they should always bear in mind the basic principles set out above, assessing whether they act as data controller or data processor.

Jargon Buster

Controller: decides how and why personal data is processed.

Processor: acts on the controller's behalf.