# The Information Commissioner's response to the HM Treasury consultation on the implementation of the revised EU Payment Services Directive II

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR). She also deals with complaints under the Re-use of Public Sector Information Regulations 2015 (RPSI) and the INSPIRE Regulations 2009. She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (the ICO) welcomes the opportunity to respond to this consultation on the implementation of the revised Payment Services Directive II (PSDII). As not all the questions in the consultation paper relate to issues within the ICO's remit, we have focussed only on those that do. We have also made some general comments about the potential interaction between the implementation of PSDII and data protection requirements.

The Consultation correctly identifies that data protection law is being reformed and we are currently in the implementation phase of the General Data Protection Regulation (GDPR) which takes effect from 25 May 2018. The Information Commissioner expects businesses to take steps during this period to ensure they are ready for GDPR, and that Government will reflect the changes when developing public policy. It is important that the implementation of PSDII does not introduce requirements that conflict with data protection obligations.

The ICO has engaged with the development of Open Banking at various stages in its development, and we encourage industry to maintain an open dialogue as it designs and implements an open API standard. The Information Commissioner views Open Banking as a key way in which individuals' rights to data portability under Article 20 of GDPR may be given practical effect, and it should therefore help financial institutions meet their data portability obligations.

**17/03/2017** Version 1.0 (final)

In order to aid understanding of our response to this consultation, it's important to appreciate that the GDPR sets a new, higher standard for "consent". For consent to be valid under GDPR, it must be:

- freely given, specific, informed and unambiguous,
- clearly distinguished in an intelligible and easily accessible form, using clear and plain language,
- indicated by a clear affirmative action,
- capable of being withdrawn, and as easy to withdraw as it is to give, and
- demonstrable i.e. organisations should keep records.

The GDPR also makes reference to "explicit consent" as a ground for processing more sensitive types of data, for example data about an individual's health, sexual orientation or racial origins. Whilst many people consider details of their income and expenditure to be especially private, they do not in themselves constitute sensitive or special categories of data. Obtaining explicit consent is also a way to legitimise automated individual decision making, including profiling. We are currently consulting on our GDPR consent guidance, but we explain in our draft guidance that explicit consent must be expressly confirmed in words, rather than by any other positive action. Therefore, even if it is obvious from an individual's actions that they consent to the processing of their personal data in a particular way, this cannot be "explicit consent" unless it is also expressly confirmed in words.

**Conduct of Business Rules**

**5.8(11) – Incorrect Unique identifiers**

In the event that a payer enters an incorrect unique identifier (e.g. the wrong sort code and account number) when sending a payment, resulting in the payment going to the wrong payee, Regulation 90(4) of the Payment Service Regulations 2017 (PSRs)[1] requires the payer's payment service provider to provide the payer with *"all available relevant information in order for the payer to claim repayment of the funds"*, in the event that the payer's payment service provider is not able to recover those funds.

[1] Which corresponds to Article 88(3) of PSDII

In these circumstances, neither the DPA nor the GDPR would prevent the disclosure of relevant personal data e.g. details of the payee who has not returned the funds they received incorrectly.

However, as this is something that an individual who did not wish to return the funds would be unlikely to freely agree to, the legal basis for processing being relied on cannot be consent as defined under GDPR. We therefore assume that any such disclosure would not be considered processing for the provision of a payment service - which, as explained below, requires the explicit consent of the payment service user.

Payment service providers will also need to clearly explain to individuals the circumstances in which their personal data will be shared with other payment service providers and/or other payment service users, what that information will be and why it will be shared. This is necessary to comply with the information requirements under Articles 13 and 14 of GDPR.

**Consent (Question 17)**

Regulation 97 of the PSRs[2] states:

*"A payment service provider must not access, process or retain any personal information for the provision of payment services unless it has the explicit consent of the payment service user to do so."*

Regulations 68, 69 and 70 of the PSRs also refer to "explicit consent". As set out above, "explicit consent" has a very specific meaning in data protection law. In this context there is a clear interaction with data protection requirements. Whilst we appreciate "explicit consent" is the term used in PSDII, care should be taken to ensure that the use of the term in this related context does not confuse or unnecessarily hamper the development of a reasonable user experience.

We also note that the term "personal information" is used in Regulation 97, as opposed to "personal data" used in Article 94 in PSDII. The term "personal data" is of critical importance in data protection law. In order to maintain consistency we would recommend that the term "personal data" is used in the PSRs.

[2] Which corresponds to Article 94 of PSDII

## Customer Authentication and security of personal data (Question 17 and Question 22)

In line with Article 98 of PSDII, the European Banking Authority (EBA) has produced a final draft of the Regulatory Technical Standards (RTS) on strong customer authentication and secure communication under PSDII. Measures implementing PSDII are expected to apply from 13 January 2018. However, it is not expected that the RTS or the security measures that payment service providers are required to take under Articles 65, 66, 67 and 97 will apply until Autumn 2018.

Both the DPA[3] and GDPR[4] require organisations to take appropriate technical and organisational measures to protect the security and integrity of any personal data that they process. Payment service providers therefore need to ensure that they have adequate systems in place to protect the security and integrity of the personal data they process as soon as they begin processing this data.

We would agree that as the draft RTS is now available, systems and procedures should be designed in line with the RTS wherever possible in order to ensure minimal disruption when the RTS eventually comes into force.

We are keen to ensure that the provisions of PSDII are implemented in a way that is harmonious with, and complements, data protection requirements. To this end, we will continue to engage with HM Treasury, the Financial Conduct Authority, industry bodies and other relevant stakeholders about this matter.

[3] Principle 7 of the DPA
[4] Article 32 of GDPR