

Process Id# :: 2111
Process Name :: EFT Bounce backs (Tullamore Control)
Date Last Updated :: 26/06/2019

Description :: Bouncebacks occurs when an invalid bank account details are provided, the money is then bounced bank to the departments bank account

Article 30 Process as carried out by the NSSO as a processor on the instruction of the PSB ::

As required under Article 30 (2) of the GDPR ::

Data Stage	Process:		Owner	Storage Location	Personal / Sensitive Data	Data Items
Data Capture/ Transfer	1	Log on to BOI Online to check for bounce backs.	EO/HEO	BOI Portal	Personal Data	Employee Name, Employee number, Pay Group, payment amount
Data Storage	2	Applicable data retrieved from BOI website and recorded on password protected excel sheet in bounce back folder on H drive under Tullamore control	EO/HEO	H Drive / OGCIO	Personal Data	Employee Name, Employee number, Pay Group, payment amount
Data Transfer	3	Email issued to payroll area to advise of bounce back and request new bank details	HEO/EO	Tullamore Control mailbox	Personal Data	Employee Name, Employee number, Pay Group, payment amount
Data Capture	4	New bank details received back from payroll/pension/T&S areas by email. Attachment of bank details should be password protected.	HEO/EO/CO	H Drive / OGCIO	Personal Data	Employee Name, Employee number, Pay Group, payment amount

Data Usage	5	Data from Step 4 used to re-direct funds, which entails logging in to BOI Portal and entering details for manual payment. 2nd person asked to verify details entered are correct before payment is authorised. 2 step process requiring 2 different people to sign off on payment on the BOI Portal	HEO/EO	BOI Portal	Personal Data	Employee Name, Address, Bank account details, Employee number, Pay Group, payment amount
Data Transfer	6	Email issued to payroll area to advise that payment has been made on instruction of previous email	HEO/EO	Outlook/ OGCIO	Personal Data	Employee Name, Employee number, Pay Group, payment amount