DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Bank Of Ireland (UK) PLC (BOI)

OF: Bowbells House
1 Bread Street
London
EC4M 9BE

1.1 The Information Commissioner (the Commissioner) issues a reprimand to BOI in accordance with Article 58(2)(b) of the UK General Data Protection Regulation (UK GDPR) in respect of certain infringements of the UK GDPR.

The reprimand

1.2 The Commissioner has decided to issue a reprimand to BOI in respect of the following infringements of the UK GDPR.

- Article 5 (1)(d) which states personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are process, are erased or rectified without delay ('accuracy').

- Article 5 (2) which states the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

1.3 The reasons for the Commissioner's findings are set out below.

1.4 BOI's parent company, BOI Group plc, was established in 1783 and is headquartered in Dublin, while BOI is a separate UK based company incorporated in 2009.

1.5 As part of its financial obligations BOI is required to and routinely reports to credit reference agencies (CRA) providing accurate information on data subjects' accounts including arrears status. The system calculates and reports the latest status including the balance owed and any default notices.

1.6 Following two data subjects raising disputes with a CRA, BOI became aware that it had sent inaccurate data to a CRA which had affected those data subject's credit profiles. Further internal investigation found that inaccurate data had also been sent to CRA for another 3,282 data subjects based in the UK between 2018 and 2020.

1.7 The investigation found that inaccurate data had only been sent to CRA's in relation to defaulted data subject's loan accounts where the account had been sold to debt collectors. This had the potential to lead to unfair refusal or granting of credit to data subjects.

1.8 Whilst data subject's personal data was correctly recorded and had not been compromised, the incorrect recording of a data subject's default loan status along with an incorrect outstanding balance led to inaccurate personal data being incorrectly held on their account.

1.9 As the selling of accounts was infrequent, BOI explained it operated a manual system and staff were required to type the appropriate system reference into the status field which would indicate the loan had been sold. Failure to do this resulted in the loan being shown as being owned by BOI with an outstanding balance. In the majority of cases the purchaser of the debt also reported the outstanding balance, which appeared on the data subject's account and therefore was recorded on the data subject's credit profile twice – a double default.

1.10 BOI explained whilst it had risk management measures in place for debt sales, the specific issue relating to the debt sold flag was not included as a granular risk. No specific assurance reviews or audits took place in relation to the debt sales flag.

1.11 BOI further explained that data subject's accounts affected in 2019 had been rectified by a local fix. However, BOI could not provide any documentary evidence, or an explanation as to why the incident was not escalated internally at the time. It also couldn't explain why a historic check on previous accounts was not carried out to identify any inaccuracies or why new processes were not put in place to prevent any future errors.

1.12 It should be noted that due to the nature of credit scoring and different factors involved which contribute to a data subject's credit scoring, it would be impossible to determine actual detriment to each data subject. However, it is reasonable to assume that due to the inaccurate recording of data subject's personal data that was sent to CRA's that some negative impact has occurred.

1.13 It should also be noted that as this incident was not a personal data security breach as defined in the UK GDPR ('the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data') BOI were under no obligation to report it to the ICO.

1.14 The investigation found that BOI failed to take reasonable steps to ensure accurate personal data was recorded with the CRA which affected 3,284 data subjects. Opportunities were missed in 2019 when corrective action was taken to rectify inaccurate data subject's credit profiles. BOI's failure to take remedial action meant 115 cases of the error continued for up to 33 months.

1.15 The investigation also found whilst BOI had risk management measures in place in relation to debt sales, it failed to identify the importance of the sold debt flag which had been included in the process as a manual step.

1.16 Furthermore, BOI failed to undertake any assurance reviews of accounts in relation to the debt sale flag or have oversight of the process. Had it had, the error could have been resolved in 2019 and further errors could have been prevented.

Remedial steps taken by BOI

1.17. The Commissioner has also considered and welcomes the remedial steps taken by BOI in the light of this incident. In particular

- BOI has informed and supported affected data subjects where it has deemed necessary.

- BOI has corrected all affected data subject's accounts.

- BOI is reviewing the end to end debt sale process to identify any weaknesses and to ensure any further issues are identified and mitigated.

- BOI has suspended its debt sales until the review of the process has taken place and appropriate processes have been put in place.

Decision to issue a reprimand

1.18. Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to BOI in relation to the alleged infringements of articles of the UK GDPR set out above.

1.19 BOI were invited to provide representations which were submitted to the ICO on 7 November 2023.

- BOI stated there was not significant challenge to the factual content of the proposed reprimand.

- BOI provided an explanation as to the structure of the Bank which is reflected in the reprimand.

- BOI confirmed that points 1 and 2 of the recommended steps to improve BOI's compliance have already been completed through a large scale remediation workstream.

- BOI also stated that it is intending to conduct a wider assurance review of all CRA reporting processes and controls across BOI UK during 2024 and is ensuring learnings from this incident are shared across the bank.

- BOI acknowledged that the ICO included in the reprimand that the infringement did not constitute a personal data breach as defined under UK GDPR and did not require notification to the ICO.

Further Action Recommended

1.19. Due to the length of time since the incident took place the following steps may have already been addressed. However, the Commissioner recommends that BOI should take certain steps to ensure its compliance with UK GDPR. With particular reference to article 5(1)(d) and Article 5 (2) of the UK GDPR the following steps are recommended:

1. Continue to provide any necessary support to help mitigate any potential detriment to the affected data subjects where applicable.

2. Assess any new processes and procedures that have been put in place as a result of this incident and the review and continue to monitor these over a period of time to ensure that they are effective and to prevent another occurrence of this incident in the future.

3. Ensure the learning from this incident is shared across the organisation - not just the departments where it occurred - to embed lessons learnt from the incident and to improve understanding and your compliance with data protection.

1.20 The ICO recognises that the BOI has already progressed with the recommended action above in order improve its compliance with UK GDPR.