Appendix A - Progress Update Against 'Urgent' ICO Recommendations

Recommendation	Agreed Action	Update for Audit Committee 15.03.22
a.4.Document where departmental risk registers exist, and commence enquiries into where they don't and why. BMBC should ensure that all departments are aware of their risk registers, and that ownership is allocated to a suitable staff member. This will mitigate the risk of misuse of personal data, and ensure BMBC are in compliance with their obligations under the UK GDPR.	A4.1 - corporate approach to risk management to be agreed A4.2 - risk management strategy to be drafted and approved a4.3 - interim information risk register to be prepared to capture current areas of risk, which will include extraction of risks from DPIAs where these are articulated	All **Complete** - A Risk Register and specific IG Risk Register have now been developed.
a.6. BMBC must implement an APD to support the accuracy of the decision made to process special category or criminal offence data. This will ensure BMBC meets the requirements of Part 3 Section 42 or Schedule 1 of the DPA18.	a6.1 - Appropriate Policy Document to be prepared and approved in line with requirements of DPA18	All **Complete** - Document produced and final draft with IGSG for approval by 07.03.22
a.16. BMBC should ensure that the categories of information set out in Article 28(3) of the UK GDPR are included in all processor contracts - consider implementing a standard contract in order to achieve this. Once contracts have been updated, BMBC should ensure that compliance	a16.1 - review of standard processor contracts to identify gaps with compliance a16.2 - amended processor contract to be developed and approved for use a16.3 - review of existing processor contracts and arrangements agreed to transfer onto new	a16.1 **Complete**. a16.2 **Complete** – information governance requirements part of all contract procurement templates

checks are carried out on updated contracts. This reduces the risk that BMBC may lose control of personal data or be unable to respond to individual rights requests within the timeframe designated by the UK GDPR. This will also ensure compliance with Article 5(2) of the UK GDPR.	contract, or amendment to contract issued and returned a16.4 - process for undertaking regular compliance checks to be agreed a16.5 - schedule for compliance checks agreed and implemented with updates reported to IGSG on quarterly basis	a16.3 and a 16.4 **Complete** – information governance compliance included in monitoring of all contracts and reviewed on annual basis a16.5 **Complete** – incorporated as standing quarterly agenda item
a.19. BMBC should ensure their RoPA contains all the information required by Article 30 of the UK GDPR, and details processing undertaken by processors. This will ensure that BMBC is conforming with Article 30.	a19.1 -gap analysis of ROPA against Article 30 to be undertaken a19.2 - ROPA to be refreshed by departments where gaps identified a19.3 - quality assurance review of ROPA to ensure it includes internal and external processing activity a19.4 - guidance materials to be provided to IAOs to support ROPA updates	a19.1 and a19.2 Review and refresh of ROPA **complete**. a19.3 **Complete** - Process developed for ROPA to be reviewed and quality assured on annual basis complete. a19.4 **Complete**
a.20. Implement a central log of lawful bases for processing for all processing activities - including details of any law, statute, or additional obligation for that processing. This could be incorporated into the RoPA, the APD, or in a separate document or record. This will provide assurance that BMBC is selecting the right basis for processing, and is compliant with Articles (5)(1)(a) and 5(2) of the UK GDPR.	a.20.1 - actions as per 1.19.1-4	a.20. **Complete**

a.23. BMBC should undertake an LIA to ensure that the interests of the controller are adequately balanced against the rights and freedoms of the data subject.	a.23.1 - gap analysis of current HR processing against Article 5(2) to be undertaken a.23.2 - Legitimate Interest Assessment to be completed	All **Complete**.
a.36.A. BMBC should update their Personal Data Breach Reporting Policy and Procedure to include the UK GDPR and DPA18, and the obligations they place on controllers regarding personal data breaches. This will ensure that BMBC has a clear, consistent approach to data breaches and can fulfil their obligations under Article 33 and 34 of the UK GDPR. B. Formulate a specific training module around data breaches and near misses. By ensuring staff have appropriate training around recognising, reporting, and preventing data breaches, BMBC will have ongoing assurance that they are maintaining compliance with Articles 33 and 34 of the UKGPDR. C. Create an area for recording near misses, effects of the breach, and remedial action taken on the Personal Data Breach Log. This will ensure that BMBC are recording breaches and near misses	a.36.a.1 - refresh of Data breach reporting policy to be undertaken to include reference to GDPR and DPA18 a.36.a.2 - Data Breach Policy to be approved and circulated to colleagues with supporting guidance which includes how to report breaches and near misses a.36.b.1 - Data breach training to be added to TNA a.36.b.2 - data breach and near miss KPIs to be agreed and reported to IGSG with trend analysis and lessons learned a.36.b.3 - bespoke data breach training material to be prepared a.36.b.4 - arrangements for monitoring attendance to be agreed and implements a.36.b.5 - training compliance to be reported to IGSG at agreed frequency	a36.a.1 and a35.a.2 – **Complete** and to receive final approval by IGSG a.35.b.1 – **Complete** – data breach training part of the corporate IG mandatory training for all staff and additional training available to all teams. a.36.b.2 – **Complete**. a.36.b.3 – **Complete** – also see a.35.b.1 above a.36.b.4 – **Complete**. DPO receives regular updates and reports to IGSG. a.36.b.5 – **Complete** – as a.36.b.4 above

appropriately, and can conduct analysis on both an individual and broad scale to inform mitigating and remedial actions.	a.36.c.1 - Data breach log to be established a.36.c.2 - data breach form to be considered for implementation to ensure all relevant information is captured a.36.c.3 - medium - longer term arrangements to be considered which best meet organisational need and reduce duplication	a.36.c.1/2/3 – **Complete**