DATA PROTECTION ASSURANCE REPORT

SYPA DPO Assurance Plan: 2019/2020
Breach Management Report

Date of Issue: *10th July 2019*

BARNSLEY
Metropolitan Borough Council

Table of Contents

Key Dates

Assurance Review Stage	Date
Pre- assurance review meeting Date:	30th April 2019
Draft Report Issued:	5th July 2019
Draft Report Discussed:	9th July 2019
Final Report Issued:	10th July 2019

Report Distribution

Name
Client Lead: Jason Bailey - Head of Pensions Admin
George Graham – Fund Director
Neil Copley – Section 151 Officer (Final Only)
Andrew Frosdick – Monitoring Officer to South Yorkshire Pensions Authority (Final Only)

DPO Assurance Team Contact Information

Name/ Role	Email/ Telephone
Rob Winter – Data Protection Officer (DPO)	RobWinter@barnsley.gov.uk 01226 773241
Louise Gething – Senior Auditor	LouiseGething@barnsley.gov.uk 01226 773190

Acknowledgement

The DPO would like to take this opportunity to express thanks to management and staff for their help and co-operation during this review.

Confidentiality

This report is strictly private and confidential and as such is for the exclusive use of the intended recipients. The content and results of the review should not be copied in part or in whole without the prior permission of the receiving sponsor of the report.

Assurance Review Methodology

The review was conducted in conformance with the Public Sector Internal Audit Standards using a combination of enquiry, observation and sample testing techniques.

Executive Summary
DPO Assurance Review – SYPA Breaches Management

Introduction and Background

General Data Protection Regulations (GDPR) and Data Protection Act (DPA) principals are at the heart of data collection, processing and sharing.

The Information Commissioner's Office (the ICO) enforces and promotes compliance with the DPA, which contains eight principles of good information handling and GDPR.

Recital 87 of the GDPR - Promptness of reporting / notification makes clear that when a security incident takes place, the authority should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Personal Data Breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Authority has to consider the likelihood and severity of the risk to people's rights and freedoms, following a breach. When this assessment is made, if it's likely there will be a significant risk then the ICO must be informed.

This review was part of **planned** DPO assurance work for 2019/20.

Assurance Review Objectives and Scope

Scope

The scope of this review was to consider the breach management arrangements for the Authority and consider whether there are sufficient procedures, controls and processes in place.

The review covered the following areas:-

- breach management policy: existence of a policy providing a framework for reporting and managing information security breaches,
- ownership and understanding of breach management responsibilities: management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security breaches,
- breach reporting and feedback procedures, including reporting to the ICO: staff should be aware of the nature of an information security event, its potential detriment to the organisation and how to report it,
- appropriate escalation of breaches: information security breaches should be responded to in accordance with the documented procedures, and
- breach logs and review of breach management systems: evidence of lessons learned and consideration by senior management.

Objectives

The Authority has a duty to establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required as per Recital 87 of the GDPR - Promptness of reporting / notification. The objective of the review was to provide assurances that there are

adequate breach reporting procedures, controls and processes in place to fulfil the Authority's responsibility in recognising, receiving, processing, recording, reporting and responding to data breaches.

DPO's Final Assurance Opinion

Based on the above the DPO can provide the SIRO with a **Substantial** assurance opinion in relation to the internal control framework.

An explanation of the ratings is included within the Glossary of Terms.

Summary of Implications

Impact	Number	Adequacy of Controls	Application of Controls	Systems Efficiency
High	0	0	0	0
Medium	0	0	0	0
Low	1	1	0	0
Total	**1**	**1**	**0**	**0**

Positive Findings

The following good practices were identified during this review:-

- ✓ A process for personal data incident reporting, investigation, recording and responding Is in place in practice and robust;
- ✓ Line Manager responsibility is in place and there is an intranet link for staff to log breaches in the shared document store (SharePoint);
- ✓ The Head of Pensions Administration is automatically informed when the log is updated;
- ✓ The breach log is shared on a quarterly basis with the Local Pensions Board and this is a regular agenda item;
- ✓ Comments about individual incidents are invited from the Board;
- ✓ The report to the Local Pensions Board includes the dates that incidents were identified, dates (when applicable) that incidents were reported to the DPO and/or the ICO.

Overall Conclusion

From the review, the DPO has made **1** implications, these have been classified as:

- High 0
- Medium 0

- Low 1
- Verbal 0

Based on the above the DPO can provide a **Substantial** assurance opinion in relation to the internal control framework. An explanation of the ratings is included within the Glossary of Terms.

The reason that a substantial rating has been given is because SYPA have a process in place with regard to personal breach management. The process is robust with line manager responsibility, a reporting log, recording of incident details and relevant dates, details of reporting to the DPO and the ICO and the sharing of this information with the Local Government Board. The current policy however does not fully align with actual practice and does not reference GDPR, the ICO, timeframes and the DPO. It may be advisable to consider a separate personal data procedure or adapt the current procedure to include these specific areas.

The following sections of the report summarise the findings of the review. Where relevant, any control weaknesses identified are outlined, including actions that have been agreed in order to address the associated risks.

Risk: The Security Incident Reporting arrangements of the Authority are inadequate and not consistent with the requirements of Recital 87 of the GDPR. Recital 87 of the GDPR - Promptness of reporting / notification makes clear that when a security incident takes place, the authority should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Breaches Management Procedures

Finding

1.1 Although there is a 'blanket' procedure for breach management which covers reportable law breaches to the Pensions Regulator, there is insufficient procedural advice in this document regarding personal information data breaches. This would include mention of the GDPR requirements, statutory timeframes, investigation responsibilities, cyber incidents and when to notify the DPO and ICO.

It may be advisable to have a separate procedure in place to document personal data breaches or adapt the existing policy.

Implication

- Although the process of incident reporting is place in practice the procedures are not tailored to cover GDPR specific requirements such as timeframes, reporting to ICO and liaison with the DPO so there is a risk that the security reporting arrangements of the authority is inadequate and not consistent with the requirements of Recital 87 of the GDPR.
- Incidents/Breaches are not promptly reported and investigated.

Control/Risk Impact Low	**Adequacy of Controls**	**Governance Theme:** Information Governance	**Risk Ref:**

Agreed Management Action (AMA)

AMA1

The existing breach management policy will be updated to explicitly reference the procedures for handling breaches in the context of GDPR, including statutory timeframes, investigation responsibilities, cyber incidents and when to notify the DPO and ICO.

It is felt, in the context of the pension's environment, it would be more beneficial to retain a single integrated policy that covers ICO and TPR requirements as the process will follow a similar decision tree and the updated procedural advice attached to the policy will reflect this. The updated policy will be presented to the Local Pension Board at their next meeting in October.

Responsible Officer:
Head of Pensions Administration

Target Implementation Date

30 September 2019

1. Classification of Implications (Impact on control/risk)

High Significant impact on ensuring the objectives of the system under review are met.

Medium Requiring action to avoid exposure to a significant risk to the achievement of the objectives of the system under review.

Low Action is advised to enhance control or improve operational efficiency.

2. Assurance Opinions

	Level	Control Adequacy	Control Application
POSITIVE OPINIONS	**Substantial**	Robust framework of controls exist that are likely to ensure that objectives will be achieved.	Controls are applied continuously or with only minor lapses.
	Reasonable	Sufficient framework of key controls exist that are likely to result in objectives being achieved, but the control framework could be stronger.	Controls are applied but with some lapses.
ADVERSE OPINIONS	**Limited**	Risk exists of objectives not being achieved due to the absence of key controls in the system.	Significant breakdown in the application of key controls.
	No	Significant risk exists of objectives not being achieved due to the absence of controls in the system.	Fundamental breakdown in the application of all or most controls.