CRANE **PENSION TRUSTEE COMPANY (UK) LIMITED**

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

CRANE PENSION TRUSTEE COMPANY (UK) LTD AND
CRANE UK GROUP LIFE ASSURANCE SCHEME (THE "SCHEME")

THE GENERAL DATA PROTECTION REGULATIONS ("GDPR")
DATA BREACH MANAGEMENT AND REPORTING POLICY

Breach Identification

- Any GDPR data breach is to be reported to the data breach team (**"DBT"**):

  Scott Dalrymple;

  sdalrymple@cranebsu.com / 00 44 1462 443230;

  Alternatively contact a member of the Trustee GDPR Sub Committee on 00 44 1473 277321.

- Examples of what a data breach is can be found at **Appendix 1** to this policy. Data breaches may be identified and notified by entities/ persons which process Scheme data, such as, third party providers.

- Once the DBT is aware of a breach, it will log the breach in writing and/ or electronically, using the Breach Register found at **Appendix 2** to this policy.

- The DBT will also communicate to the person reporting the breach:

  - That the breach has been acknowledged by the DBT;

  - That steps will be taken to investigate the breach and to ascertain the nature of the breach and to whom it needs to be reported; and

  - Whether further information is required regarding the breach. The DBT will liaise with the reporter of the breach to investigate the breach, its cause, its extent and its likely impact and consequences.

- As part of its investigations, the DBT will assess whether the event reported is in fact a data breach and not a "near miss".

Breach Notification

- The DBT will consider whether notification of the breach is required (or ought) to be made to any third parties. The DBT will notify the breach to:

  - The Information Commissioner's Office (**ICO**) where the breach is likely (in the DBT's view) to result in a risk to the rights and freedoms of individuals.

When assessing the risk to individuals, consideration will need to be given to the circumstances of the breach, including the likelihood, severity and potential impact of the risk. The following factors should be considered when assessing the risk:

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

- Type of breach;
- Nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of the individual (e.g. children or other vulnerable individuals may be at greater risk); and
- Number of individuals affected.

An example where a breach is unlikely to result in such a risk may be where the personal data is already publicly available and therefore the disclosure of the data does not constitute a further risk to the individual.

Any notification to the ICO must be made without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Where notification has not taken place within 72 hours, reasons for the delay will be provided to the ICO.

Any notification to the ICO will be provided in the standard form set out at **Appendix 5** to this policy. The notification will include an outline of the steps to be taken in order to prevent any future breaches in the short term and of any changes in policy or actions to be undertaken as a result of the current breach.

Accompanying guidance notes from the ICO on breach notifications are set out at **Appendix 5** to this policy.

  - An individual (i.e. data subject) where the breach is likely to result in a *high* risk to the individual's rights and freedoms.

This is a higher threshold than for determining whether notification should be made to the ICO. Where notification to an individual is required, notification to the ICO will always be required.

The factors described above should be considered when determining whether notification of a breach needs to be made to an individual.

Any notification to an individual should be made without undue delay (i.e. as soon as possible).

Before any notification to a data subject is made, the DBT will advise the Trustee (and the member's employer, if such an individual is still an employee) of the intention to notify the data subject.

The DBT will make any such notification in the form at **Appendix 4** to this policy. The notification will include an outline of the steps to be taken in order to prevent any future breaches in the short term and of any changes in policy or actions to be undertaken as a result of the current breach.

- If it is not clear whether to notify the breach to the ICO and/ or to an individual or individuals, the DBT will seek legal advice.
- The DBT will also consider whether any other third parties ought also to be notified of the breach (e.g. third party providers to the Scheme). A list of third parties and their roles in relation to the Scheme is attached to this policy at **Appendix 3**.

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

Breach Prevention

- The DBT will consider any steps that need to be taken to prevent any further breaches. Depending on the circumstances, this may involve (but is not limited to):
    - Liaising with third party providers to the Scheme as to the steps they are and/ or should be taking to prevent any further breach;
    - Consideration of whether or not to change encryptions to Scheme personal data or to add or strengthen passwords applicable to the access of Scheme personal data;
    - Considering the individuals who are able to access Scheme personal data and whether access needs to be restricted further;
    - Considering whether any data ought to be destroyed (this may need to be considered alongside the Trustee's **Retention Policy**);
    - Considering whether there is a need to stop or limit any form of processing of Scheme personal data as a precautionary measure as a result of the breach (e.g. if there is a concern that the processing may result in a further or recurrent breach);
    - Considering whether any changes need to be made to security measures in place for the processing of personal data and whether new security measures need to be introduced; and
    - Considering whether any additional training is required for any party involved in the breach.

Breach Register and Report

- On completion of the investigation, the DBT should record the following in the Breach Register (at **Appendix 2** to this policy):
    - The date of notification of the breach;
    - The description and nature of the breach – this will include the dbt's record as to whether it accepts that a breach has occurred (and that the event is not a "near miss");
    - The personal data affected by the breach;
    - To whom the breach has been notified and when. If the breach has not been notified to the ico or affected individuals, the reason for such a decision should be recorded;
    - The identified cause of the breach; and
    - The steps taken to resolve the breach and mitigate the potential for any further breach.

CRANE **PENSION TRUSTEE COMPANY (UK) LIMITED**

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

APPENDIX 1

BREACH EXAMPLES

The below events are examples of breaches of the GDPR:

- **"Confidentiality breach"** - where there is an unauthorised or accidental disclosure of, or access to, personal data
    - This could include someone who is not one of the Trustee directors or authorised by the Trustee accessing data, data being communicated accidentally (such as sending an email to the incorrect email address) or a document being lost or left somewhere accidentally
    - It could also include electronic devices being lost or stolen, such as laptops, mobile phones, tablets and USB drives, or a conversation in which a data subject is discussed being overheard by a third party
- **"Availability breach"** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data
    - A breach under this heading could be temporary, such as a power or other infrastructure failure, or could be a permanent loss of, or unscheduled destruction of, personal data
- **"Integrity breach"** - where there is an unauthorised or accidental alteration of personal data
    - This category includes any change that is made to personal data which is unintentional or unauthorised – this could include malicious hacking or even, for example, accidentally overwriting part of a spreadsheet with incorrect data or sorting data incorrectly in a file so that the records for individuals are changed.

CRANE **PENSION TRUSTEE COMPANY (UK) LIMITED**

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

APPENDIX 2

CRANE PENSION TRUSTEE COMPANY (UK) LTD AND
CRANE UK GROUP LIFE ASSURANCE SCHEME

GENERAL DATA PROTECTION REGULATIONS: BREACH REGISTER

DATE BREACH NOTIFIED	DESCRIPTION/ NATURE OF BREACH	PERSONAL DATA AFFECTED	DATE ICO FORM SUBMITTED If not submitted, provide reasons why	DATE INDIVIDUAL NOTIFICATION FORM SUBMITTED If not submitted, provide reasons why	CAUSE OF BREACH	MITIGATING ACTIONS

CRANE **PENSION TRUSTEE COMPANY (UK) LIMITED**

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

APPENDIX 3

CRANE PENSION TRUSTEE COMPANY (UK) LTD AND
CRANE UK GROUP LIFE ASSURANCE SCHEME (THE "SCHEME")

LIST OF THIRD PARTIES

The following parties have involvement with the Crane Pension Trustee Company (UK) Ltd and Crane UK Group Life Assurance Scheme (the "Scheme")
and have, or have access to, data for which the Scheme trustee is data controller:

Name of Party	**Role in relation to the Scheme**
Conduent	Pension Administrator and Actuary
Equinity	Pension Administrator and Actuary (UMC)
Ensors	Payroll provider and auditor
Legal & General	Pension and AVC provider
Scottish Widows	Pension provider
Crane Fund	Member financial support
Deloitte	Crane Auditor
Crane Co	Internal Auditor
Clerical Medical	AVC provider
Prudential	Pension provider
Equitable Life	AVC provider
Standard Life	AVC provider
Aviva	Pension and AVC provider
HM Revenue & Customs	Data Controller

CRANE

PENSION TRUSTEE COMPANY (UK) LIMITED

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

APPENDIX 4

CRANE PENSION TRUSTEE COMPANY (UK) LTD AND
CRANE UK GROUP LIFE ASSURANCE SCHEME (THE "SCHEME")

GDPR – PERSONAL DATA BREACH
INDIVIDUAL NOTIFICATION FORM

Date of Breach		**Date Breach Identified**	
Breach Detail	Nature of the personal data breach		
	Data affected		
	Consequences/risks		
Contact	Scott Dalrymple – Sdalrymple@cranebsu.com / 00 44 1462 443230 or alternatively contact a member of the Trustee GDPR Sub Committee on 00 44 1473 277321.		
Measures Taken/Proposed	Measures to address the personal data breach		
	Measures taken or proposed to mitigate adverse effects		
	Suggested actions		*[include here suggestions for actions that individuals can take to protect their data, for example changing their passwords, checking accounts, changing their security questions]*

CRANE **PENSION TRUSTEE COMPANY (UK) LIMITED**

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

APPENDIX 5

CRANE PENSION TRUSTEE COMPANY (UK) LTD AND
CRANE UK GROUP LIFE ASSURANCE SCHEME (THE "SCHEME")

GDPR – PERSONAL DATA BREACH
ICO NOTIFICATION FORM

Date of Breach		**Date Breach Identified**[1]	
Breach Detail	Nature of the personal data breach, including prevailing circumstances and causes/reasons		
	Categories and approximate number of data subjects concerned		
	Categories and approximate number of personal data records concerned		
Contact	Scott Dalrymple – Sdalrymple@cranebsu.com / 00 44 1462 443230 or alternatively contact a member of the Trustee GDPR Sub Committee on 00 44 1473 277321.		
Likely Consequences	[*describe the likely consequences of the personal data breach*]		
Measures Taken/Proposed	Measures to address the personal data breach		
	Measures taken or proposed to mitigate adverse effects		
	Details of Data Protection policies relevant to the breach being reported		

[1] Where the report is being made more than 72 hours after the breach was identified, reasons must be provided for the delay.

CRANE **PENSION TRUSTEE COMPANY (UK) LIMITED**

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

ico.
Information Commissioner's Office

Data protection breach notification form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, e.g. incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

(a) * What is the name of your organisation – is it the data controller in respect of this breach?

(b) Please provide the data controller's registration number. Search the online Data Protection Public Register.

(c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

2. Details of the data protection breach

(a) * Please describe the incident in as much detail as possible.

(b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Personal data placed at risk

(a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

CRANE HOUSE,
EPSILON TERRACE, WEST ROAD,
IPSWICH, SUFFOLK, IP3 9FJ
enquiries@cranebsu.com
www.cranebsu.com

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form

• Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)