Knorr-Bremse (UK) Executive Scheme
Data Protection, Privacy and Information Security Policy

1 INTRODUCTION

In the ordinary course of administering and managing the Knorr-Bremse (UK) Executive Scheme (the "**Plan**") the trustees (the "**Trustee**") collects, hold, process and transfers personal data relating to members of the Plan ("**Members**") and other beneficiaries in receipt of benefits from the Plan such as Members' dependants ("**Beneficiaries**").

The Trustee recognises the importance of establishing and operating a very high standard of data protection for personal data, as failure to do so can have serious legal implications and may, for certain breaches of European Data Protection Legislation, result in the imposition of a fine of up to €20 million.

The Trustee is the data controller (as defined under European Data Protection Legislation) for any information that it collects from Members and Beneficiaries in connection with administering the Plan. This Data Protection, Privacy and Information Security Policy (the "**Policy**") relates to the handling and processing of all Members' and Beneficiaries' personal data, whether held manually or electronically, and sets out the minimum standards of conduct and procedure the Trustee expects for the handling of Members' personal data in compliance with the European Data Protection Legislation.

2 DEFINITIONS

For the purposes of this Policy, "European Data Protection Legislation" is defined as, for the periods in which they are in force, the European Data Protection Directive 95/46/EC, all laws giving effect or purporting to give effect to the European Data Protection Directive 95/46/EC (such as the Data Protection Act 1998) or otherwise relating to data protection (to the extent the same apply) and, from 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/670) (GDPR) or any equivalent legislation amending or replacing the GDPR.

3 SCOPE

3.1 Who does this Policy apply to?

This Policy applies to the Trustee and to each individual trustee. The Trustee will also have regard to this Policy in its dealings with its advisers, suppliers, the Scheme's sponsoring employer and other third parties including but not limited to other companies in the sponsoring employer's group.

Failure to adhere to this Policy may result in civil or criminal legal action being taken against the Trustee by data protection authorities or by the individuals to whom the personal data relates.

3.2 What does the Policy relate to?

The processing of Member personal data. Processing means:

- carrying out any operation or set of operations on the data;
- collecting, recording or holding data; and
- use of the data which includes but is not limited to transferring, amending, consulting, sharing, storing, archiving and even destroying it.

3.3 What is Member personal data?

Any information relating to a Member or Beneficiary from which such Member or Beneficiary can be identified, directly or indirectly, or from which, with other information, they can be identified. These identifiers may include the Member's name, address, date of birth, an identification number such as a National Insurance number, health data, an online identifier or one or more factors specific to the physical, psychological, mental, economic, cultural or social identity of that Member.

It makes no difference where the data is held, e.g. whether it is in a computer database, on e-mails, or on paper in a filing system of such a type that the data is readily obtainable.

4 CORE PRINCIPLES OF THIS POLICY

4.1 Data Protection Laws

It is essential that each individual trustee:

- complies with this Policy;
- understands and observes any data protection laws applicable, including the European Data Protection Legislation; and
- ensures that Members' and Beneficiaries' personal data is handled with appropriate confidentiality and security.

4.2 Collection and Use of Personal Data

The Trustee collects personal data in many ways, including but not limited to, from Members and Beneficiaries (or their IFA) directly; from application forms completed by

Members on joining the Plan; from a Member's employer; from expression of wish forms completed by the Member; from information provided in relation to potential beneficiaries on the death of a Member, from track and trace services and from HMRC and other law enforcement agencies. The data is collected and processed for the purpose of:

- calculating and paying benefits;
- administering the Plan;
- managing the Plan (as a whole and Members' membership of it) by the Trustee and any third party to whom the Trustee has delegated obligations arising in connection with Members' and Beneficiaries' benefits;
- carrying out obligations arising from any contracts entered into between Members and their employer and to provide Members with any information they request from the Trustee;
- analysis by the Trustee and, to the extent necessary, any other organisation required (such as the Trustee's external advisors, including legal advisers, and the Trustee's insurers or potential insurers);
- communicating with Members and Beneficiaries about their pension by mail, telephone, email, text or other electronic means;
- complying with the Trustee's auditing and/or reporting requirements;
- complying with legal and regulatory requirements or to protect the rights, property or safety of the Trustee, the Members and Beneficiaries, or others; and
- complying with the Trustee's legal obligations, resolving disputes and enforcing the Trustee's rights.

The underlying principles for the collection and use of personal data are that:

- it should be processed fairly and lawfully. Personal data will be collected and processed only for legitimate needs relating to the Plan, used only for purposes that are known to the Members and Beneficiaries, and kept confidential. Where data is to be disclosed to a third party outside the Plan, or transferred outside the European Economic Area ("**EEA**"), Members should be made aware of this.
- it should be adequate, relevant, and not excessive. No more data should be gathered than is needed - personal data should not be gathered or held "just in case".

- it should be accurate and kept up to date. Personal data should be correctly recorded, and updated promptly when appropriate. Procedures and control must be in place to ensure that this is achieved.

- it should be kept no longer than necessary, or as required by law.

4.3 Rights of the Individual

It is the Trustee's policy to respect the rights of Members and Beneficiaries and to provide them with reasonable access to data held.

The Trustee will provide Members and Beneficiaries with written information about the data it controls and how they should exercise their rights in relation to it through issuing them with a Fair Processing Notice. The Trustee issued an updated Fair Processing Notice on its website in June 2022 (*and advised members in the Summary Funding Statement 2022 issued in June 2022*) and will re-issue such notices where appropriate. The Trustee acknowledges that it may also control personal data in relation to certain former Members of the Plan (e.g. those who have transferred their benefits from the Plan) but as it can no longer be certain that it holds up-to-date addresses for such persons, it has decided it would be disproportionate to send Fair Processing Notices to them.

At their written request, Members and Beneficiaries will be provided with a copy of their personal data held by the Trustee unless any such data can be legitimately withheld. The Trustee may request a fee only where appropriate in accordance with the European Data Protection Legislation, for example, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

If necessary the Member or Beneficiary making the request may be asked to prove his/her identity and may also be asked to provide information to enable the data in question to be located. The information should be provided as soon as is practicable and in any event within 30 days of the Member or Beneficiary making the request although this can be extended by a further 2 months if the request is particularly complex or a large number of requests are received by the Trustee.

Furthermore, at their written request, the information can be provided to Members and Beneficiaries in a way that makes it easy for a computer to read.

Members and Beneficiaries should be permitted to correct or update the information as necessary.

Members and Beneficiaries also have the right to ask the Trustee to delete or remove any personal data it holds in relation to them if:

- the personal data is no longer necessary for the administration and management of the Plan;

- they have withdrawn their consent to processing and consent was the only legal basis on which the Trustee was entitled to process the data (e.g. potentially in relation to the processing of health data where the Trustee has no other lawful basis for processing such data);

- they have objected to the processing and there is no overriding legitimate interest for continuing the processing.

The Trustee can refuse a request from a Member or Beneficiary for his data to be deleted where the data is required to comply with a legal obligation e.g. in case of enquiries from HMRC or where it may be needed for the exercise or defence of legal claims. If the Trustee is unsure as to whether it should comply with such a request it should seek legal advice.

4.4 Special Categories of Personal Data

Special categories of personal data (formerly known as sensitive data) is information on a Member's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, physical or mental health, data concerning health or sex life and sexual orientation, criminal convictions and offences or related security measures that is not carried out under the control of official authority, genetic data and biometric data.

The collection and processing of special categories of personal data is very strictly regulated generally requiring the freely given, specific, informed and unambiguous consent of Members and Beneficiaries (unless processing is necessary to carry out the Trustee's legitimate interests, for example, to make a determination in connection with a Member or Beneficiary's eligibility for benefits payable under the Plan and even then only where the Trustee has an enforceable data protection policy which sets out how such data is retained and erased).

It is the Trustee's policy to collect special categories of personal data only when absolutely necessary, for example, when considering an application for an ill-health early retirement pension or determining eligibility for a lump sum or spouse's pension following a Member's death.

Special categories of personal data must be made available to users only on a strict "need to know" basis, and managed with the highest practical level of security and confidentiality. For details of the Trustee's security and confidentiality measures, see section 5 below.

4.5 Disclosure of Personal Data

It is the Trustee's policy to ensure that personal data relating to Members and Beneficiaries is protected at all times, and it is the responsibility of all users of personal data to ensure that data is treated confidentially. The Trustee may share Members' and Beneficiaries' personal data with the Member's employer, other participating employers in the employer group, other companies in the employer's group, the scheme administrator and the Trustee's professional advisors and service providers to the extent that it is necessary for the management and administration of the benefits provided by the Plan.

The Trustee may share Members and Beneficiaries' personal data with selected third parties including but not limited to:

- when specifically asked to do so by the Member or the Beneficiary e.g. to an independent financial adviser;
- in the event that the sponsoring employer sells or buys any business or assets, in which case the Trustee may disclose Members' or Beneficiaries' personal data to the prospective seller or buyer of such business or assets and their advisors;
- in the event that the Trustee considers de-risking or insuring any of the benefits provided by the Plan in which case the Trustee may disclose Members' or Beneficiaries' personal data to prospective insurers and/or its or the sponsoring employer's advisers;
- if the Trustee is under a duty to disclose or share Members' and Beneficiaries' personal data in order to comply with any legal obligation or to protect the rights, property or safety of the Trustee, or others. This may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

The Trustee does not use Members and Beneficiaries' personal data for marketing purposes or transfer personal data to other organisations for the purpose of marketing their goods or services.

When the Trustee shares personal data with third parties, such third party will process Members or Beneficiaries' data as either a data controller or as the Trustee's data processor and this will depend on the purpose of the Trustee's sharing of the data.

Where personal data is disclosed to third parties who will be processing data controlled by the Trustee it must be done so in accordance with European Data Protection Legislation. In such circumstances:

- the Trustee must ensure that third parties are reliable, that they will keep data confidential, and that they have adequate technical and organisational security arrangements in place;

- a contract must be in place that binds the third party to the same obligations as apply to the Trustee, and under which the third party agrees to act only in accordance with instructions from the Trustee, and to take adequate technical and organisational security measures when processing personal data; and

- no more data should be provided than is necessary for the performance of the contract.

The personal data that the Trustee collects from Members and Beneficiaries may be transferred to, and stored at, a destination outside the EEA to the extent that it is necessary for the management and administration of the benefits provided by the Plan. It may also be processed outside the EEA by the Trustee's advisers or suppliers. In compliance with the European Data Protection Legislation, should Members' and Beneficiaries' personal data be transferred to, and stored at, a destination outside the EEA the Trustee will take all steps reasonably necessary to ensure that such data is safeguarded through adequate means, such as ensuring that the recipient has entered into Standard Contractual Clauses approved by the European Commission.

Those who process data controlled by the Trustee are:

Mercer Ltd. as scheme administrator;

Knorr-Bremse Systems for Commercial Vehicles Ltd. as payroll provider;

The Trustee has confirmed that its sharing of personal data with its data processors, including the above, complies with the requirements set out in this section 4.5 and in section 4.6 below.

In addition, the Trustee's advisers include the following who are data controllers in their own right and will, therefore, be directly responsible for complying with European Data Protection Legislation when processing any personal data relating to the Plan's Members and Beneficiaries:

Mercer Ltd. as scheme actuary;

Burges Salmon as legal adviser;

Knorr-Bremse Rail Systems (UK) Ltd. as participating employer;

Those who process data controlled by the Trustee outside the EEA are directly contracted by Mercer Ltd. and subject to same compliance as above.

Again, the Trustee has confirmed that its sharing of personal data with such third parties complies with the requirements set out in this section 4.5 and in section 4.6 below.

4.6 Data Security

The Trustee ensures that risk appropriate technical and organisational measures are in place to prevent unauthorised or unlawful processing and accidental loss, disclosure, destruction, damage or access to personal data, whether in the Trustee's possession or in the possession of third parties. Please see section 5 of the actions the Trustee takes to ensure the security of Members and Beneficiaries' personal data when in its possession.

The Trustee will also take reasonable steps to safeguard the accuracy and completeness of personal data, whether in the Trustee's possession or in the possession of third parties.

The Trustee ensures that data processors use, adopt and continue to comply with appropriate technical and organisational security measures. The Trustee ensures that:

- it is satisfied that data processors are clear about their responsibilities and that it has been provided with any written policies on the data processors' record keeping processes;
- it is clear about what data processors will, and will not, do for it and what information they need from it;
- it is satisfied that any information it needs from data processors is readily available so that it can meet its other legal and regulatory responsibilities;
- it informs data processors promptly about any changes in order that they can keep their records up to date;
- it is satisfied that it is kept informed of any problems data processors encounter with maintaining scheme records, or would be kept informed if any were to arise;
- any personal data sent by data processors to trustees is encrypted, anonymised or pseudonymised; and
- records are kept on the systems of the Plan's administrator from time to time for as long as it takes to provide the pension and other benefits provided under the rules of the Plan and for such period afterwards as necessary to comply with the Trustee's legal obligations, resolve disputes and enforce its rights.

Any data processors whose document destruction policies include the destruction of paper records once they have been converted to electronic images, must confirm that they have processes in place to ensure that any documentation destroyed does not

include the Plan's governing documentation, signed contracts, agreements, deeds and statutory declarations.

5 TRUSTEE PRACTICE TO ENSURE SECURITY OF PERSONAL DATA

Each individual trustee will comply with the following technical and organisational measures to aim to prevent the unauthorised or unlawful processing and accidental loss, disclosure, destruction, damage or access to personal data. The golden rule is to respect the privacy of the Members and the Beneficiaries to whom the data relates and to treat their data as highly confidential. This means that each individual trustee will:

- comply with this Policy in all respects at all times;
- only record information which is necessary and not use it for purposes which have not been communicated to Members and Beneficiaries in the Trustee's Fair Processing Notice;
- not provide information unless it is certain the recipient is who they say they are and that they have a valid justification for receiving the data;
- provide only the data necessary to fulfil the purpose for which it is required by the recipient;
- not provide information over the telephone, fax, or in any other way, if the Trustee is not certain who will receive it. If in doubt, the Trustee will not give the information;
- ensure that the Trustee has explicit consent to process special category personal data or that it has another lawful basis for processing such data; and
- ensure that special category personal data is kept even more securely, with access strictly limited, and used only for the approved purpose. The Trustee will not collect such data unless it is essential to do so.

The only personal data relating to Members and Beneficiaries that each individual trustee has access to:

- relates to individual Member cases (e.g. relating to death or ill-health cases) which the scheme administrator sends to the Trustee in a password protected file;
- is contained within meeting papers issued by the scheme administrator as part of the hard copy meeting pack sent by signed for post.

Elementary housekeeping to ensure the security and confidentiality of such personal data is vital. In particular each individual trustee will:

- ensure that access to any personal data stored electronically is password protected, and keep passwords confidential;
- ensure that manual data and files are secure at all times, for example in a locked filing cabinet or locked drawer;
- not leave information unattended, whether paper records or unattended computer screens;
- ensure that personal data records are accurate and up-to-date, and that unnecessary and outdated records are deleted/destroyed;
- not print personal data if it is not essential to do so, and ensure that printouts are shredded and disposed of properly when no longer needed. In particular, the trustee will ensure they do not keep any hard copies of individual Member cases or of any meeting packs at home (unless redacted) and will shred or return any such material to the scheme administrator once the individual case has been considered;
- not forward or share any materials containing personal data except to the Trustee's advisers, other trustees or to reply to the sender of the email;
- delete emails containing personal data (along with any attachments) as soon as they have been actioned;
- not allow anyone else access to their email account (including family members and other trustees) although the trustee may use the same email address for Trustee business as for other purposes;
- take appropriate measures to ensure the security of their mobile phone, tablet or personal computer as the case may be. In particular, each trustee will ensure that such devices are password-protected and consider functionality to remotely wipe data if a device is lost or stolen;
- not store, upload or download any personal data from or to secure cloud services or run unofficial apps or use unauthorised services, such as Dropbox, Google Drive or similar;
- before accessing personal data from outside the EEA, consider whether such access is really necessary.

If any trustee has any queries regarding how to ensure the security of their systems, they should speak to the sponsoring or participating employer's IT Department.

6 DELETION AND DESTRUCTION OF DOCUMENTS

The Trustee will consider, on a regular basis, whether it is necessary to retain certain records. In doing so, the Trustee recognises that pensions are long-term investment vehicles and it is not uncommon for queries or disputes to arise in relation to Members' and Beneficiaries' benefits years after a Member has left the service of his employer or even after a pension has been put into payment. However, once a Member or Beneficiary's pension has been put into payment or a Member has transferred his pension out of the Plan, the Trustee will take steps to ensure that access to such personal data is limited by arranging for it to be stored in an archive to which access is limited.

Each trustee will ensure they do not keep any hard copies of personal data at home (unless redacted) and will shred or return any such material to the scheme administrator once the individual case has been considered. Where hard copies of personal data are to be destroyed, the Trustee will always use a shredder or confidential waste bag.

If any trustee has any doubt as to whether it is appropriate to delete or destroy a particular document, they will ask the Chairman of Trustees who will decide the appropriate course of action.

7 REPORTING BREACHES

Breaches of this Policy, whether actual or suspected, must be reported by individual trustees to the Chair of Trustees or, in his absence, to a person designated by the Chair of Trustees to receive such reports, within 24 hours of becoming aware of a breach. The Chair of Trustees will then investigate and consider what action should be taken, having obtained legal advice if required.

Where there has been a breach of European Data Protection Legislation the Chair of Trustees must notify the Information Commissioner's Office without undue delay and where feasible no later than 72 hours after the relevant individual trustee first became aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The Chair of Trustees should submit the report electronically to casework@ico.org.uk or on the Information Commissioner's Office website, and retain a copy of the notification.

Where a breach of European Data Protection Legislation is likely to result in a high risk to the rights and freedoms of individuals, the Trustee must also write to any affected individuals to notify them of the breach without undue delay. Should the Chair of Trustee

have any doubt as to whether a particular breach is likely to result in a high risk to the rights and freedoms of individuals, they should seek legal advice.

8 COMPLIANCE WITH THIS POLICY

The Trustee will review this Policy periodically or when there are circumstances that merit an earlier review. It will monitor compliance with this Policy through its Risk Register.

As part of its Trustee training programme all individual trustees will be provided with data protection and security training within 6 months of appointment. Refresher training will also be provided to individual trustees as appropriate.

The Trustee is not required to have a Data Protection Officer under European Data Protection Legislation as it is not a public sector organisation, its core activities do not require the regular and systematic monitoring of data subjects on a large scale nor does its core activities require the processing of special category data and data relating to criminal convictions and offences. It has decided, therefore, not to appoint one.

Should an individual trustee have any queries in relation to this Policy, they should contact the Chair of Trustees in the first instance.

Policy created: March 2018
Policy last reviewed: March-June 2022