| Approved by:<br>M. Stansfield<br>Managing Director | NMB<br>MinebeaMitsumi Group<br>United Kingdom<br><br>Human Resources Policy | NMB-HR-POL109<br><br>Effective Date:<br>19.06.26 |
|---|---|---|
| **Subject: Data Protection Policy** | | |

**Data Protection Officer:**

Alison Robinson
NMB-Minebea UK Ltd
Doddington Road
Lincoln
LN6 3RA
Tel +44 (0)1522 500933

## INTRODUCTION

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

## DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, eg a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Data subject" is any identried or identifiable natural person, whose personal data is processed by the controller responsible for the processing.

"Processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination restriction, erasure or destruction.

"Restriction of processing" is the marking of stored personal data with the aim of limiting their processing in the future.

"Profiling" means any form of automated processing or personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Pseudonymisation is the processing or personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Controller" responsible for the processing is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"Processor" is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"Recipient" is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those

public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

"Third party" is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"Consent" of the data subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

## DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- processing will be fair, lawful and transparent
- data will be collected for specific, explicit and legitimate purposes
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
- data will be kept accurate and up to date
- data which is found to be inaccurate will be rectified or erased without delay
- data is not kept for longer than is necessary for its given purpose
- data will be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- we will comply with the relevant GDPR procedures for international transferring of personal data.

## TYPES OF DATA HELD

We keep several categories of personal data on our employees to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, eg our holiday booking system.

Specifically, we hold the following types of data:

- personal details such as names, addresses, phone numbers
- information gathered via the recruitment process such as that in a CV or included in a cover letter, references from former employers, details on your education and employment history, etc
- details relating to pay administration such as National Insurance numbers, bank account details and tax codes
- medical or health information
- information relating to your employment with us, including:
    - job title and job descriptions
    - your salary
    - your wider terms and conditions of employment
    - details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
    - internal and external training modules undertaken.

All the above information is required for our processing activities. More information on those processing activities is included in our privacy notice for employees, which is available from your manager.

**EMPLOYEE RIGHTS**

You have the following rights in relation to the personal data we hold on you:

- the right to be informed about the data we hold on you and what we do with it
- the right of access to the data we hold on you (more information on this can be found in the section headed "Access to Data" below and in our separate policy on subject access requests)
- the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected ("rectification")

- the right to have data deleted in certain circumstances ("erasure")
- the right to restrict the processing of the data
- the right to transfer the data we hold on you to another party ("portability")
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

## RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

## LAWFUL BASES OF PROCESSING

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's consent to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

## ACCESS TO DATA

As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a subject access request. We will comply with the request without delay and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded or excessive, or unless a request is made for duplicate copies to be provided to the employee making the request or to a third party acting on the employee's behalf. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

## DATA DISCLOSURES

The Organisation may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals — whether any reasonable adjustments are required to assist them at work
- individuals' health data — to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration — to consider how an individual's health affects their ability to do their job
- the smooth operation of any employee insurance policies or pension plans
- to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

## DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner, so they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs,

laptops, etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Organisation's rules on data security may be dealt with via the Organisation's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

## THIRD-PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Organisation's commitment to protecting data.

## INTERNATIONAL DATA TRANSFERS

The Organisation does not transfer personal data to any recipients outside of the EEA.

## REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In

addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

## TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection, data protection complaints and the actions to take upon identifying a potential data breach.

The nominated data— *controller* for the Organisation are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security and to understand the consequences to them as individuals and the Organisation of any potential lapses and breaches of the Organisation's policies and procedures.

## RECORDS

The Organisation keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities