MIB Job Applicant Data Privacy Notice

Status	Version 1.0
Issued	May 2018
Document owner	Head of HR
Document author	Head of HR
Key purpose of paper	To provide information to job applicants on how we process their data
Decisions required	N/A

Contents

1 About this data privacy notice

1.1 This notice is designed to provide information on how Motor Insurers' Bureau (referred to as "we", "us", "our") processes the personal data of job applicants (referred to as "you", "your") who apply to us for a job.

1.2 As a "data controller", we are responsible for deciding how we process personal data about you. We take your privacy seriously and we are fully committed to protecting your personal data at all times. We will only process your personal data in accordance with, and adhere to the principles (as applicable) contained within, the General Data Protection Regulation and, when enacted, the Data Protection Act 2018 (together referred to as the "GDPR").

1.3 This notice does not form part of any offer of employment and we may amend it at any time to reflect any changes in the way in which we process your personal data. If you are in the application process when any changes or updates are made to this notice, we will bring any such changes to your attention as soon as is practicable. We may also notify you in other ways from time to time about the processing of your personal data.

1.4 Our Data Protection Officer ("DPO") is responsible for ensuring that this privacy notice is maintained and shall oversee questions in relation to this notice. The DPO post is held by Kaushik Patel (Chief Risk Officer) who can be contacted at GDPREnquiries@mib.org.uk or 01908 830001.

2 The kind of information we hold about you

2.1 "Personal data" is any information about a living individual from which they can be identified such as name, ID number, location data, any online identifier (such as IP address), or any factor specific to the physical, physiological, genetic, mental, economic or social identity of that person. It does not include data where any potential identifiers have been removed (anonymous data) or data held in an unstructured file.

2.2 There are "special categories" of more sensitive personal data which are more private in nature and therefore require a higher level of protection, such as genetic data, biometric data, information about sex life or sexual orientation, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health.

2.3 When we refer to "processing", this means anything from collecting, using, storing, transferring, disclosing, altering or destroying personal data.

3 How we use your personal data

3.1 We process your personal data for various reasons, relying on a variety of different bases for lawful processing under the GDPR as set out below.

3.1.1 To comply with our legal obligations or exercise legal rights conferred upon us. This may include:

- checks for eligibility to work in the UK as required by immigration laws, such as passport and visa documentation;
- formal identification documentation relating to you, such as a passport or driving licence, to verify your identity (including your date of birth); and
- Disclosure and Barring Service (DBS) checks where we have a legal right or reason for doing so (for further information see section 5 below).

3.1.2 To pursue our (or a third party's) legitimate interests as a business. This may include:

- your contact details such as your name, address, telephone number and personal email address which will be used to communicate with you in relation to the recruitment process;
- your CV, any education history, employment records, professional qualifications and certifications in order for us to consider your suitability for the job you are applying for;
- details of the job role you are applying for any interview notes made by us during or following an interview with you, in order to assess your suitability for that role;
- pay and benefit discussions with you to help determine whether a job offer may be made to you;
- For certain roles given the sensitive nature of the business and for the prevention of fraud and to protect the security of the data we hold, information relating to any county court judgment check, bankruptcy check, directorship check, basic disclosure check (through Disclosure Scotland) proof of address check, HM Treasury Sanctions List check, Financial Services Register check, Motor Insurance Database check, an insurance history check using NetReveal (claims and policy data) and a full security clearance check carried out by Defence Vetting Agency;
- voicemails, emails, correspondence, and other communications created, stored or transmitted by you on or to our computer or communications equipment in order to progress the application through the recruitment process;
- CCTV footage of you onsite in Linford Wood House consists of external cameras positioned to overlook the car parks and exterior of the building. Other cameras and proximity sensors have been installed internally and in stairwells and public spaces (like the reception and corridors).

- In Noble House, CCTV is restricted to cameras being located in the internal domain of MIB leased areas and not to stairwells or reception / atrium areas or corridors. The CCTV is in place for security reasons, for the protection of our property and for health and safety reasons.
- In Sackville House, CCTV is restricted to cameras being located at the front and rear doors; and
- network and information security data in order for us to take steps to protect your information against loss, theft or unauthorised access.

3.2 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

4 How we use your special categories data

4.1 We also collect, store and use your special category personal data for a range of reasons, relying on a variety of different bases for lawful processing under the GDPR, as set out below.

4.1.1 To enable us to perform our legal obligations in respect of employment, social security, social protection law, or needed in the public interest. This may include:

- health information to assess and/or to comply with our obligations under the Equality Act 2010 (for example a requirement to make reasonable adjustments to your working conditions).

4.1.2 For occupational health reasons or where we are assessing your working capability, subject to appropriate confidentiality safeguards. This may include:

- information about your physical or mental health, or disability status, to assess whether any reasonable adjustments are required for you during the recruitment process, carrying out any medical assessment required for your role, pension and any insurance benefits.

4.1.3 To establish, defend or exercise legal claims in an employment tribunal or any other court of law.

4.1.4 For statistical purposes in the public interest such as equal opportunities monitoring (for example the collection of information about race, ethnic origin, sex or religion). Any such information shall only be used, once collected, in an anonymised form for statistical purposes and will not be not used in relation to your application for employment with us.

5 Information about criminal convictions

5.1 We will hold information about criminal convictions.

5.2 We will only collect this information if it is appropriate given the nature of your role and where the law allows us to do so. This will usually be where such processing is necessary to carry out our data asset management obligations, provided that we do so in line with our Data Protection Policy. We may collect this information as part of the recruitment process and during the employment relationship or we may be notified of such information directly by you in the course of you working for us. For details on how long we retain criminal convictions information and how it is disposed of, please refer to Appendix One.

6 If you fail to provide personal information

6.1 If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications, work history or background check information), we will not be able to process your application successfully. For example, if we require a credit check or references for a role and you fail to provide us with relevant details, we will not be able to take your application further.

7 Automated decision making/profiling

7.1 We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

8 Data sharing

8.1 We may share your personal data and special category personal data internally. In particular, it may be shared with: HR employees involved in the recruitment process, employee relations and/or administration of your employment; line managers; consultants; advisers; and/or other appropriate persons who may be involved in the recruitment process for the job(s) you are applying for.

8.2 We may share your personal data and special category personal data with other companies within our group of companies. They may use your personal data as part of our regular reporting activities on performance or for systems maintenance support and hosting of data.

8.3 We may share your personal data and special category personal data with third parties, agents, subcontractors and other organisations (as listed below) where we have a lawful basis for doing so:

Category of personal information	Recipient/relationship to us	Purpose of disclosure
All personal information collected	IT service providers	To support, maintain and host our information systems, including the software and hardware infrastructure required for it to operate/be accessible online and to keep a backup of your personal information. We also use online IT service providers to provide contract execution services
All personal information collected	Our legal and other professional advisers (including accounting and audit services)	To provide us with advice in relation to our business, including our legal, financial and other obligations and claims
Name, date of birth and contact details	Background/employee vetting provider	To check suitability of and/or ensure the safety and security of data help by MIB on behalf of the insurance industry
All personal information collected	Recruitment agencies	To assist with recruitment into our organisation
Job role and health data	Occupational health providers	For working capacity of worker to be assessed
All personal information collected	Provider of employee benefits	To enrol the employee and possibly their dependants into benefits provided by MIB

8.4 When we disclose your personal data to third parties, we only disclose to them any personal data that is necessary for them to provide their service. We have contracts in place with third parties in receipt of your personal data requiring them to keep your personal data secure and not to use it other than in accordance with our specific instructions.

8.5 When we disclose your personal data to third parties, they may disclose or transfer it to other organisations in accordance with their data protection policies. This does not affect any of your data subject rights set out at 13 below. In particular, where you ask us to rectify, erase or restrict (the processing of) your personal data, we have an obligation to ensure that this instruction is passed on to any third parties whom we have disclosed your personal information to.

8.6 All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

8.7 We may also share your personal data and special category personal data with other third parties for other reasons. For example: in the context of the possible sale or restructuring of the business; to provide information to a regulator; or to otherwise comply with the law. To comply with our legal obligations, we may share your data with the following:

- HMRC for tax purposes; and
- Home Office for immigration purposes

8.8 We may obtain personal data and/or special category personal data about you from third party sources, such as recruitment agencies, job boards, recruitment assessment centres, occupational health professionals and background check providers. Where we receive such information from these third parties, we will only use it in accordance with this notice.

8.9 In some cases, they will be acting as a controller of your personal data and therefore we advise you to read their privacy notice and/or data protection policy.

9 Transferring information outside the EEA

9.1 We do not envisage that we will transfer your personal data outside of the EEA (meaning the EU 27 member states, the UK, Norway, Iceland and Liechtenstein), however we will notify you in writing if this position changes.

10 Data storage and security

10.1 Your personal data and special category personal data is stored in a variety of locations, including: electronically on our secure servers/in hard copy form in access-restricted or locked filing cabinets.

10.2 We take appropriate technical and organisational security measures and have rules and procedures in place to guard against unauthorised access, improper use, alteration, disclosure and destruction and accidental loss of your personal data.

10.3 In addition, we limit access to your personal data to those who have a business need to know and they will only process your personal data on our instructions and subject to a duty of confidentiality.

10.4 We have put in place procedures to deal with any suspected or actual data security breach and will notify you and the Information Commissioner's Office ("ICO") of a suspected breach where we are legally required to do so.

10.5 Whenever we propose using new technologies, or where processing is construed as 'high risk', we are obliged to carry out a data protection impact assessment which allows us to make sure appropriate security measures are always in place in relation to the processing of your personal data.

11 Data Retention

11.1 We keep your personal data and special category personal data for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Information about how long we retain such personal data is set out in Appendix 1.

11.2 When applying for a job with us, we compile and keep a manual and/or electronic file containing information about you which relates to your application for a job with us. Your information will be kept secure and will be used for the purposes of your job application, as explained above.

11.3 If you are offered and you accept a job with us, your personal data will be transferred to a manual and/or electronic personnel file. Any hard copy personnel file will be kept in access-restricted, locked filing cabinets.

11.4 In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use and retain such information without further notice to you, as it falls outside of the definition of personal data under the GDPR.

12 Your duties

12.1 We encourage you to ensure that the personal data that we hold about you for the purposes of your application or for the purposes of considering you for any similar roles is accurate and up to date by keeping us informed of any changes to your personal data. You can update your details by emailing Hum

13 Your rights

13.1 You may make a formal request for access to personal data and/or special category data that we hold about you at any time. This is known as a Subject Access Request. Such a request must be made in writing and we must respond within 1 month. Please note that under the GDPR we are permitted to extend the 1 month time period for responding by an additional 2 months where in our view your request is complex or numerous in nature. We may also charge a reasonable fee based on administrative costs where in our view your request is manifestly unfounded, excessive or a request for further copies. Alternatively, we may refuse to comply with the request in such circumstances. For further details on subject access requests please contact the Risk and Compliance department at DSARdept1@mib.org.uk, or for details on the types of request listed below, please contact the Risk and Compliance department at GDPREnquiries@mib.org.uk.

13.2 Under certain circumstances, by law you also have the right to:

13.2.1 have your personal data corrected where it is inaccurate;

13.2.2 have your personal data erased where it is no longer required. Provided that we do not have any continuing lawful reason to continue processing your personal data, we will make reasonable efforts to comply with your request;

13.2.3 have your personal data be transferred to another person in an appropriate format;

13.2.4 withdraw your consent to processing where this is our lawful basis for doing so;

13.2.5 restrict the processing of your personal data where you believe it is unlawful for us to do so, you have objected to its use and our investigation is pending, or you require us to keep it in connection with legal proceedings; and

13.2.6 to object to the processing of your personal data, where we rely on legitimate business interests as a lawful reason for the processing of your data. You also have the right to object where we are processing your personal data for direct marketing purposes. We have a duty to investigate the matter within a reasonable time and take action where it is deemed necessary. Except for the purposes for which we are sure we can continue to process your personal data, we will temporarily stop processing your personal data in line with your objection until we have investigated the matter. If we agree that your objection is justified in accordance with your rights, we will permanently stop using your data for those purposes. Otherwise, we will provide you with our justification as to why we need to continue using your data.

13.3 The way we process your personal data and the lawful basis on which we rely to process it may affect the extent to which these rights apply. If you would like to exercise any of these rights, please address them in writing to the DPO.

13.4 We may need to request specific information from you to help us to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

13.5 In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. If you withdraw your consent, our use of your personal data which was collected before your withdrawal is still lawful.

13.6 You have the right to complain to a supervisory body if you are concerned about the way we have processed your personal data. In the UK this is the ICO – www.ico.org.uk.

13.7 Although you have the right to complain to the ICO, we encourage you to contact us first with a view to letting us help in resolving any queries or questions.

14 Questions

14.1 If you have any questions about any matter relating to data protection or the personal data and/or special category personal data that that we process about you, please contact the DPO.

15 Appendix 1

Data category	Retention Period	Reason	Disposal
Job applications and interview records of candidates	12 months – unless following an unsuccessful application you specifically consent to us holding it for longer for the purpose of contacting you in the event that any similar jobs / roles become available from time to time.	To defend against potential legal claims	Securely destroyed by shredder / third party document destruction company and electronic documents deleted.
Criminal Records Information (such as DBS check results)	For unsuccessful applicants any DBS checks would be destroyed within 6 months following the outcome of the recruitment exercise.	To comply with the DBS code of practice issued under section 122(2) of the Police Act 1997	Securely destroyed by shredder / third party document destruction company and electronic documents deleted.