M&G plc Speak Out Guidelines

Speak Out Guidance Note

Data Protection & Privacy

Speak Out is the scheme by which people can raise an issue. It may or may not be a protected disclosure under applicable employment laws and/or regulations. This guidance is intended to apply to all staff (where-ever located), with the General Data Protection Regulation 2016 ("GDPR") and the UK Data Protection Act 2018 to be viewed as setting the standard. In setting this standard attention is drawn that there may be differences depending on, amongst other things, where you are located. You should seek local advice to understand your all your rights as additional data privacy laws and investigation rules may also apply.

This guidance seeks to explain how your data will be used during this process and who will see it/have access to it.

What constitutes Personal Data?

The GDPR defines 'Personal data' as:

'*any information relating to an identified or identifiable natural person (a 'data subject').'*

This legal definition is intentionally wide and includes any personal identifier(s) relating to a natural person who can be identified, directly or indirectly, in particular by reference to that identifier such as a name, an identification number (e.g. staff ID), location data (e.g. address), online identifiers or contact information (e.g. email and/or telephone number).

1.1 Personal Data collected when raising a reportable concerns:

When utilising any of the reporting mechanisms outlined in Section 4 of the M&G Speak Out Guidelines, (or via *NAVEX),* you may need to provide the following types of personal data will likely be requested:

- Your name;
- and
- Contact information (e.g. telephone number or an email address)

From time to time, you may also be required to share "Special Category" personal data to further outline the nature of the incident. This includes more sensitive information about an individual(s) which reveals or results in the processing of any or all of the following:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;

- biometric data for the purpose of uniquely identifying a natural person;
- anything related to a person's health; or
- a person's sex life or sexual orientation.

In addition to this, you may be required to disclose or report other types of information which, whilst not strictly "Special Category" by definition, remains, nonetheless, highly sensitive in nature such that extra care and consideration around managing this information is required at all times (e.g. ensuring the highest levels of confidentiality and security). Further, it is important that any information you provide is always up-to-date and accurate to facilitate the provision of a comprehensive and compliant Speak Out investigation Programme.

1.2 Data Controller

The M&G plc group includes a number entities that are registered as data controllers and who are required to collect and use ('process') personal data on behalf of M&G plc in connection with the Speak Out programme (together "M&G").

M&G takes its legal responsibilities as data controller seriously, including with respect to whistleblowing. For example, when you provide personal data to us in the context of the 'Speak Out' programme, we will collect, store and use this data because it is absolutely necessary to do so to ensure compliance with, for example regulatory rules and specifically to discharge our regulatory requirements under the FCA's Handbook (SYSC 18). Your information will be recorded and shared with a restricted group of employees engaged to handle sensitive information.

1.3 Lawful Basis

Processing personal data to ensure compliance with regulatory rules such as the FCA rules also means, for example, that M&G will have an appropriate and recognised 'lawful basis' to process your data. Processing under a 'lawful basis' (also known as a 'condition for processing') is a strict legal and mandatory requirement under data protection legislation. When processing personal data for the purposes of whistleblowing, M&G currently relies on the lawful basis set out under Article 6(1)(c) of the GDPR together with the condition for processing set out under Schedule 9 of the Data Protection Act 2018. In particular, under Schedule 9, sub-section 3 where:

- The processing is necessary for compliance with a legal obligation to which the controller is subject, other than an obligation imposed by contract.

Where M&G is required to process "Special Category" personal data (see section 1.1 above), an additional 'lawful basis' or 'condition for processing' is required, due to the much higher sensitivity of the data involved. In such circumstances, M&G currently relies on the additional lawful basis set out under Article 9(2)(g) of the GDPR, together with the condition for processing set out under Schedule 8 of the Data Protection Act 2018, specifically, at sub-section 1 where processing of personal data:

- is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and
- is necessary for reasons of substantial public interest.

Further details of how and why M&G processes your personal data, including for legal and regulatory purposes, can be found in our privacy notices, available on the *PeopleHub* (Search for "Privacy Notices").

From time to time, M&G may seek to rely on provisions contained in the Data Protection Act 2018, which may provide exemptions from data subject rights and data controller obligations in certain circumstances.

You are reminded that where reporting a whistleblowing incident from outside the United Kingdom you should seek advice as to impact of local laws and legislation in this area.

1.4 Processing by third party controllers

To the extent you provide or discuss whistleblowing information directly with a third-party (e.g. *NAVEX* or *Protect*), they, in turn, will have similar legal responsibilities as data controllers to process your data lawfully.

1.5 Your rights

As an individual data subject, you are ordinarily afforded a number of automatic legal rights under data protection legislation. For example, the right to be informed (of the processing of your data) or to make a data subject "access request" or "DSAR" (to access your information).

In order to preserve the integrity of the Speak Out programme, and to discharge its regulatory duties, M&G may seek to rely on provisions contained in the Data Protection Act 2018. For example, the Data Protection Act provides a limited number of exemptions to M&G from meeting certain obligations it would ordinarily need to fulfil, as data controller.

1.6 Security

M&G takes the security of all data it holds very seriously. We have an Information Security and Technology Risk Policy including an established and detailed Information Security framework with policies, standards and controls, aligned to recognised International Standards including ISO27001 and NIST.

Given that the information processed may be sensitive and that leaks or unauthorised disclosure may have adverse consequences, both for the whistle blower and the persons accused or implicated, special care must be taken at all times to ensure appropriate technical and organisational measures are in place to mitigate risks around confidentiality, information loss or mis-use and to ensure data and information security. For

example, when sharing or receiving information under the programme you should follow the advice given , to ensure that information remains secure at all times and does fall into the wrong hands.

1.7 Sharing your personal information outside the UK or EU/EEA

We do not anticipate needing to transfer your personal data outside of the UK or Europe for the purpose of reporting whistleblowing incidents. However, to the extent this applies, please refer toour privacy notices available on the *PeopleHub* (Search for "Privacy Notices"). For whistleblowing cases or incidents reported in countries across Europe or further afield, additional rules around international data transfers may apply and you may need to seek local advice.

1.8 M&G Data Privacy Team

If you need advice or have questions relating to the processing of your personal data, including your data protection rights, please contact the data privacy team at the email address set out below.

Email: Data.Privacy@Prudential.co.uk

V3.0 22 MAY 2020