Motorola Solutions

Controller United Kingdom Binding Privacy Rules

Introduction

These United Kingdom Controller Binding Privacy Rules ("**Rules**") explain how the Motorola Solutions group ("**Motorola Solutions**") as a controller respects the privacy rights of its customers, staff, suppliers and other individuals whose personal information Motorola Solutions collects, uses and transfers from the United Kingdom ("**UK**").

All companies within the Motorola Solutions group of companies ("**Group Members**") and their staff must comply with these Rules as controllers when collecting or using any personal information which is protected under UK data protection laws. Group Members transfer personal information to other Group Members on a global basis as part of Motorola Solutions' regular business activities and the Rules will apply to all Group Members as controllers when such transfers from the UK take place, including where such transfers are to another Group Member receiving the personal information as a controller or as a processor on behalf of the transferring controller.

The Rules seek to ensure that personal information will be treated in a consistent, secure manner and with full respect for privacy rights and freedoms, no matter where it comes from or how Motorola Solutions uses it.

Motorola Solutions' management is fully committed to ensuring that Group Members and Motorola Solutions staff comply with these Rules at all times. Motorola Solutions staff who do not comply with their responsibilities under these Rules may be subject to disciplinary action, up to and including termination of their employment or contract.

February 14, 2022

The Rules form part of Motorola Solutions' comprehensive information security strategy and demonstrate Motorola Solutions' strong commitment to protecting individuals' privacy rights.

For an explanation of some of the terms used in these Rules, like "**controller**", "**process**", and "**personal information**", please see the section headed "Important terms used in these Rules" at the end of these Rules.

Scope of the Rules

These Rules apply whenever Motorola Solutions collects or uses personal information of staff, customers, suppliers and other individuals. They apply to all worldwide processing of personal information by Group Members as a controller, including where such transfers are either directly to another Group Member receiving the personal information as a controller or as a processor on behalf of the transferring controller or indirectly (where the personal information passes in transit through United Kingdom) to such other Group Member.

The Rules apply to all electronic personal information collected by Motorola Solutions and also to certain non-electronic personal information contained in readily accessible filing systems.

These Rules apply to all personal information that we process as controllers irrespective of the country in which the Group Member is located. The personal information processed by Group Members is described in Annex 8 (Material Scope of the BCR).

Compliance with local law

Motorola Solutions must comply with, and have a lawful basis consistent with, the requirements of applicable data protection laws when collecting and/or using personal information. Where there are no applicable data protection laws, or the law does not meet the standard set out in the Rules, Motorola Solutions will process personal information in accordance with the Rules. Where applicable data protection laws exceed the standards set out in the Rules we must comply with those laws.

Transparency and fairness

Motorola Solutions will use appropriate means to explain to individuals in a clear and comprehensive way how their personal information (collected either directly or indirectly) will be used within the time period described in Appendix 2 ("**Fair Information Disclosure**") subject to any permitted exceptions from this requirement and which are described in Appendix 2 ("**Fair Information Disclosure**").

The information Motorola Solutions will provide to individuals will include the information described in Appendix 2.

The Fair Information Disclosures shall be provided in writing, or by other means, including, where appropriate, by electronic means. They may be provided orally, at the request of an individual, provided that the identity of that individual is proven by other means.

In certain limited cases, we may not need to provide the Fair Information Disclosures, as explained in Appendix 2. Where this is the case, the Data Protection Officer must be informed and will decide what course of action is appropriate to protect the individual's rights, freedoms and legitimate interests.

Special category personal data

Unless Motorola Solutions has another lawful basis for doing so consistent with the requirements of applicable data protection laws, Motorola Solutions will only use special category personal data where the individual's explicit consent has been obtained.

When obtaining an individual's consent to use special category personal data, that consent must be given freely, and must be explicit, specific, informed and unambiguous.

Data Transfers outside the UK

Due to the global nature of Motorola Solutions' business, Group Members may transfer personal information to Motorola Solutions' ultimate parent company, Motorola Solutions,Inc. located in the United States, and to other Group Members in other countries globally that may not provide a level of protection equivalent to the laws provided in the UK.

However, Motorola Solutions must ensure that, even where this is the case, the personal information of staff, customers, suppliers and other individuals whose personal information is collected and used by Motorola Solutions as a controller will only ever be treated in accordance with these Rules.

Purpose limitation

Motorola Solutions shall collect and use personal information only for the specified, explicit and legitimate purposes notified to individuals by Fair Information Disclosures. Motorola Solutions shall not process the personal information in a way incompatible with those purposes unless the individuals are made aware of such change and have provided consent or it is in accordance with applicable law.

Motorola Solutions may have a lawful basis for processing the information for a different or new purpose, for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, taxation purposes, legal proceedings or where otherwise required to protect individuals or the rights and freedoms of others.

In particular, a Group Member may only process personal information (including special category personal data) collected in the UK for a different or new purpose if that Group Member has a lawful basis for doing so consistent with UK law.

In assessing whether any processing is compatible with the purpose for which the personal information was originally collected, we must take into account:

- any link between the purposes for which the personal information was originally collected and the purposes of the intended further processing;

- the context in which the personal information was collected, and in particular the reasonable expectations of the individuals whose personal information will be processed;
- the nature of the personal information, in particular whether such information may constitute special category personal data;
- the possible consequences of the intended further processing for the individuals concerned; and
- the existence of any appropriate safeguards that we have implemented in both the original and intended further processing operations.

Data quality, proportionality and storage limitation

Motorola Solutions will ensure that personal information collected and used is:

- accurate and, where necessary, kept up-to-date;
- adequate, relevant and limited to the purposes for which it is processed;
- not processed in a form which permits identification of individuals for longer than necessary for the purposes for which it is obtained and further processed; and
- retained in accordance with Motorola Solutions' Records Management Policy and relevant schedules, as amended from time to time.

Motorola Solutions must take every reasonable step to ensure that personal information that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Transfers to third parties

Motorola Solutions will not transfer personal information to third party data controllers or data processors outside Motorola Solutions without ensuring adequate protection for the information.

For personal information initially subject to UK data protection laws when the personal information is transferred (or onward transferred) to third party data controllers or data

processors outside of the UK, this might be achieved as permitted by UK data protection laws, including where the transfer of personal information:

- Is to a country or international organization where the relevant UK government authorities or the Information Commissioner's Office has decided that the country, a territory or one or more specified sectors within that country or the international organization in question ensures an adequate level of protection;
- Is subject to appropriate safeguards including binding corporate rules, standard data protection clauses adopted by the relevant UK government authorities or the Information Commissioner's Office and approved by the UK government authorities, Information Commissioner's Office approved codes of conduct or certification mechanisms; and/or
- Falls within a permitted condition for transfers of personal information or is otherwise subject to a derogation specified under UK data protection laws.

Publication of the Rules

Motorola Solutions will make a copy of the Rules available via a publicly-accessible website at www.motorolasolutions.com.

Rights of access, restriction, rectification, portability, erasure and blocking of personal information collected, used and transferred from the UK

Individuals whose personal information is collected and/or used in the UK and transferred between Group Members under the Rules have the right to obtain the information which relates to them and which is being processed by Motorola Solutions.

Motorola Solutions will deal with such requests in accordance with Appendix 3 (Data Subject Rights Procedure).

Staff, customers and suppliers may request to receive their personal information in a structured, commonly used and machine-readable format and to transmit that information to another controller (the right of portability), if certain grounds apply.

Motorola Solutions staff may request the restriction, erasure or rectification of their personal information, portability of their personal information and/or object to the processing of their personal information by contacting their managers or HR representatives in writing or verbally or otherwise in accordance with Appendix 3 (Data Subject Rights Procedure). Their managers and HR representatives will, in consultation with regional privacy personnel and, where necessary, the Privacy & Data Security Compliance Committee, make any necessary decision regarding such requests.

Motorola Solutions customers and suppliers may request the restriction, erasure or rectification of their personal information, portability of their personal information and/or object to the processing of their personal information by contacting Motorola Solutions at privacy1@motorolasolutions.com or otherwise in accordance with the Data Subject Rights Procedure (see Appendix 3). The Group Member with custody over the information requested will make any decisions in relation to such requests in consultation with regional privacy personnel. Where necessary, Group Members will also seek the advice of Motorola Solutions' Privacy & Data Security Compliance Committee.

The right to object to receiving marketing information

Individuals may opt out of personal data processing for purposes of direct marketing by Motorola Solutions on request and free of charge by contacting Motorola Solutions at privacy1@motorolasolutions.com.

Automated individual decisions

Motorola Solutions will ensure that where any evaluation of or decision about individuals which significantly affects them is based solely on automated processing of personal information (including profiling), those individuals will have the right to know the logic involved in the decision and appropriate measures will be taken to safeguard their legitimate interests.

We will not make any decision, which produces legal effects concerning an individual or that similarly significantly affects him or her, based solely on the automated processing of that individual's personal information, including profiling, unless such decision is:

- necessary for entering into, or performing, a contract between a group member and that individual;
- authorized by applicable law (which, for personal information protected by UK data protection laws, must be UK law); or
- based on the individual's explicit consent.

In the first and third cases above, we must implement suitable measures to protect the individual's rights and freedoms and legitimated interests, including the right to obtain human intervention, to express his or her view and to contest the decision.

Motorola Solutions will not make automated individual decisions about individuals using their special category personal data unless they have given explicit consent or another lawful basis applies.

Security and Confidentiality of Data

Motorola Solutions is committed to protecting the confidentiality, security and integrity of personal information.

To this end, Motorola Solutions will implement appropriate technical and organizational measures to protect personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves transmission of personal information over a network, and against all other unlawful forms of processing. In particular, Motorola Solutions will deploy enhanced security measures whenever processing any special category personal data. Motorola Solutions will also ensure that their staff at all times adhere to Motorola Solutions' specific information security policies in place from time to time and process personal information only on instructions from Motorola Solutions and under a duty of confidence.

Motorola Solutions has strict rules which must be complied with when using a service provider and which should be referred to when a service provider is engaged. These rules provide that Motorola Solutions will ensure that providers of services to Motorola Solutions will also adopt appropriate security measures and will enter into contractual arrangements with Motorola Solutions which require the service provider to:

- only act on the instructions of Motorola Solutions when processing that information, including with regard to international transfer of personal information;
- have in place appropriate technical and organizational security measures to safeguard the personal information;
- ensure that any individuals who have access to the data are subject to a duty of confidence;
- only engage a sub-processor if Motorola Solutions has given prior specific or general written authorisation, and on condition the sub-processor agreement protects the personal information to the same standard required of the service provider;
- assist us in ensuring compliance with our obligations as a controller under applicable data protection laws, in particular with respect to reporting data security incidents and responding to requests from individuals to exercise their data protection rights;
- assist us in ensuring compliance with our security obligations under applicable data protection laws and with notification of personal data breaches to the Information Commissioner's Office, communication of personal data breaches to data subjects, data protection impact assessments and consultation with the Information Commissioner's Office regarding data protection impact assessments;
- return or delete the personal information once it has completed its services; and
- make available to us all information we may need in order to ensure compliance with these obligations.

Where one Group Member processes personal information on behalf of another Group Member, that Group Member will adhere to the Motorola Solutions security policies in place from time to time in respect of that processing and act only on the instructions of the Group Member on whose behalf the processing is carried out. In relation to any such processing the respective Group Members shall put in place the contractual requirements described above as required for non-Group Member service providers.

When we become aware of a data security incident that presents a risk to the personal information that we process, we must immediately inform the Security Operations Center and / or the Privacy team and follow our data security incident management policies.

The Security Operations Center and/or the Privacy team will review the nature and seriousness of the data security incident and determine whether it is necessary under applicable data protection laws to notify the Information Commissioner's Office and/or individuals affected by the incident. The Data Protection Officer shall be responsible for ensuring that any such notifications, where necessary, are made in accordance with applicable data protection law.

Motorola Solutions will document in the case of any data security incident that present a risk to the personal information that we process, the facts relating to the incident, its effects and the remedial action taken.

Training Program

Motorola Solutions will provide appropriate training on the Rules and related policies in accordance with the Privacy Training Program (see Appendix 6) to all individuals who:

- have permanent or regular access to personal information including special category personal data;
- are involved in the collection of personal information; or
- are involved in the development of tools used to process personal information.

Audit Program

Motorola Solutions will conduct regular audits of compliance with the Rules (“Privacy Audits”).

Privacy Audits shall have as their scope the auditing of compliance with all aspects of the Rules and will include methods of ensuring that corrective actions take place.

The Motorola Solutions Privacy & Data Security Compliance Committee shall conduct periodic Privacy Audits. The Privacy and Data Security Committee may also conduct an unscheduled Privacy Audit more frequently in response to a specific request from a Group Member, regional privacy personnel, IS, or Motorola Solutions' management.

In addition, as part of its standards of internal control, the Motorola Solutions Audit Services department will undertake independent assessments on risk management, controls, and governance processes. Compliance with the BCR will be assessed by Audit Services using a risk-based approach.

Audit findings will be reported to the appropriate regional privacy personnel and the Privacy & Data Security Compliance Committee. Any material audit findings will be reported to the Board of Motorola Solutions.

Data Protection Impact Assessments

Where required by UK data protection laws, we must carry out data protection impact assessments (DPIA) whenever the processing of personal information, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. Motorola Solutions will carry out a DPIA prior to processing which will contain at least the following:

- A systematic description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the privacy rights of individuals;
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with applicable data protection laws.

Where the DPIA indicates that the processing would still result in a high risk to individuals, Motorola Solutions will consult with Information Commissioner's Office where required by applicable data protection laws.

Records of Data Processing

Motorola Solutions must maintain a record of the processing activities that we conduct in accordance with UK data protection laws. These records should be kept in writing (which may be in electronic form) and we must make these records available to the Information Commissioner's Office upon request.

The privacy team is responsible for ensuring that such records are maintained.

Data Protection by Design and by Default

When designing and implementing new products and systems which process personal data, we must apply data protection by design and by default principles. This means we must implement appropriate technical and organizational measures that:

- are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to protect the rights of individuals and meet the requirements of applicable data protection laws ("**privacy by design**"); and
- ensure that, by default, only personal information which are necessary for each specific processing purpose are collected, stored, processed and are accessible; in particular, that by default personal information is not made accessible to an indefinite number of people without the individual's intervention ("**privacy by default"**).

Internal Complaint Mechanisms

Any individual whose personal information is subject to these Rules may raise any privacy-related compliance questions, issues or concern that Motorola Solutions is not complying with the Rules or applicable data protection law by contacting privacy1@motorolasolutions.com. Individuals can also raise a complaint in accordance with our Complaint Handling Procedure set out in Appendix 4.

Individuals may obtain a copy of the Rules and the intra-group agreement entered into by Motorola Solutions in connection with the Rules on request to the privacy team at privacy1@motorolasolutions.com

Responsibility for breaches by non-UK Group Members

Motorola Solutions UK Limited will be responsible for ensuring that any action necessary is taken to remedy any breach of these Rules by a non-UK Group Member.

In particular:

- If an individual can demonstrate damage it has suffered likely occurred because of a breach of these Rules by a non-UK Group Member, Motorola Solutions UK Limited will have the burden of proof to show that the non-UK Group Member is not responsible for the breach, or that no such breach took place;
- Where a non-UK Group Member fails to comply with this Controller Policy, individuals may exercise their rights and remedies above against Motorola Solutions UK Limited and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Motorola Solutions UK Limited for any material or non-material damage suffered as a result of a breach of these Rules.

Shared liability for breaches with processors

Where Motorola Solutions has engaged a third-party processor to conduct processing on its behalf, and both are responsible for harm caused to an individual by processing in breach of these Rules, Motorola Solutions accepts that both Motorola Solutions UK Limited and the processor may be held liable for the entire damage in order to ensure effective compensation of the individual.

Mutual assistance and cooperation with the Information Commissioner's Office

Each Group Member shall cooperate and assist other Group Members as necessary to handle a request or complaint from an individual or an investigation or inquiry by the Information Commissioner's Office in accordance with the Cooperation Procedure (see Appendix 5).

Each Group Member shall cooperate with the Information Commissioner's Office in accordance with the Cooperation Procedure (see Appendix 5).

Relationship between UK data protection laws and the Rules

Where a Group Member has reason to believe that local legislation is likely to have a substantial adverse effect on its ability to fulfill its obligations under the Rules or has a substantial adverse effect on the guarantees provided by the Rules, the Group Member should promptly inform Motorola Solutions UK Limited and the Privacy & Data Security Compliance Committee at privacy1@motorolasolutions.com (except where prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). Motorola Solutions UK Limited and the Privacy & Data Security Compliance Committee will determine a suitable course of action aimed at ensuring compliance with these Rules in consultation with the Information Commissioner's Office (except where prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In the event of such a prohibition relating to a request received from a law enforcement authority or state security body to disclose personal information, the provisions of Appendix 7 (Government Data Request Policy) shall apply.

Third party beneficiary rights for UK Data Subjects and Liability

This section "Third party beneficiary rights for UK Data Subjects and Liability" applies where individuals' personal information are protected under UK data protection laws (including the UK General Data Protection Regulation). This is the case when:

- those individuals' personal information are processed in the context of the activities of a Group Member (or its third-party processor) established in the UK;

- a non-UK Group Member (or its third-party processor) offers goods and services (including free goods and services) to those individuals in the UK; or
- a non-UK Group Member (or its third-party processor) monitors the behaviour of those individuals, as far as their behavior takes place in the UK;

and that Group Member then transfers those individuals' personal information to a non-UK Group Member for processing under this Controller Policy.

Where this section applies, staff, contractors, clients and other individuals whose personal information is used and/or collected by a Group Member as a controller will have the right to enforce the following sections of these Rules:

- Transparency and Fairness
- Special Category Personal Data
- Data Transfers outside the UK
- Purpose Limitation
- Data quality, proportionality and storage limitation
- Transfers to third parties
- Publication of the Rules
- Rights of access, restriction, rectification, erasure and blocking of personal data collect, used and transferred from the UK
- The right to object to receive marketing information
- Automated individual decisions
- Security and confidentiality of data
- Records of data processing
- Internal Complaint Mechanisms
- Responsibility for breaches by non-UK Group Members
- Shared liability for breaches with processors
- Mutual assistance and cooperation with the Information Commissioner's Office
- Relationship between UK data protection laws and the Rules
- Third party beneficiary rights for UK Data Subjects and Liability
- Government Requests for Disclosure of Personal Information
- Data Protection by Design and Default

In addition, where this section applies, individuals may exercise the following rights:

- *Complaints:* Individuals may make complaints to the Group Member in the UK that used, collected and/or transferred their personal information and/or to the Information Commissioner's Office in accordance with the Complaints Handling Procedure at Appendix 4;
- *Proceedings:* Individuals may bring proceedings against transferred Group Member in accordance with the Complaints Handling Procedure at Appendix 4; and/or
- *Liability:* Individuals may seek appropriate redress from Motorola Solutions UK Limited including the remedy of any breach of the Rules by any Group Member outside the UK and, where appropriate receive compensation from Motorola Solutions UK Limited for any damage suffered as a result of a breach of the Rules by a Group Member in accordance with the determination of the court or other competent authority. For more information please see the Complaints Handling Procedure at Appendix 4.

Compliance and supervision of compliance

As part of its commitment to ensuring compliance with the Rules and to respecting individuals' rights to privacy, Motorola Solutions has a Privacy & Data Security Compliance Committee, a global Data Protection Officer and a network of regional privacy personnel, who take responsibility for privacy-related matters across the various functional groups (HR, Information Security, Legal, Marketing, Government Affairs and Procurement). The functional representatives consult and coordinate with one another as required. They are advised by the Data Protection Officer and are accountable to the Privacy and Data Security Committee which, in turn, is accountable to the Appointed Vice President, Ethics and Compliance, and Chief Administrative Office. At the individual country level, Motorola Solutions has trained and designated data privacy champions including a UK privacy point of contact, who is responsible for tracking compliance with country privacy laws, with support from regional legal representatives and/or the privacy team including the Motorola Solutions Data Protection Officer.

Motorola Solutions' Privacy and Data Security Compliance Committee, Data Protection Officer and extended regional privacy team must ensure that Motorola Solutions is in compliance with the Rules, as well as all applicable national and international legal and regulatory privacy requirements that relate to data privacy. In addition, the Privacy and Data Security Committee, the Data Protection Officer and regional privacy personnel are responsible for the following:

- working with business units, the Chief Administrative Office (CAO) and other core functions for the development and maintenance of policies and standards relating to data protection;
- working with the Law Department to stay current on all national and international legal and regulatory requirements that affect Motorola Solutions;
- providing data protection advice to the business units on a day-to-day and project basis;
- assisting with Information Commissioner's Office' requests for information or cooperation and managing local requests for information held about them by individuals and complaints.

Effective date of the Rules and the procedure for updating the Rules

Motorola Solutions will promptly communicate any changes to the Rules which would affect the level of the protection offered by the Rules or otherwise significantly affect the Rules (such as to the binding character of the Rules) to the Information Commissioner's Office and non-material changes will be communicated to the Information Commissioner's Office at least once a year. Motorola Solutions will also provide a brief explanation of the reasons for any notified changes to the Rules.

Motorola Solutions will communicate any changes to the Rules to the Group Members bound by the Rules and to the individuals who benefit from the Rules.

The data protection point of contact nominated by Motorola Solutions UK Limited will maintain an up to date list of the Group Members, will keep track of and record any updates to the Rules and provide the necessary information to data subjects or the Information Commissioner's Office on request. Motorola Solutions UK Limited will ensure that all new Group Members are bound by the Rules and can deliver compliance with the Rules before a transfer of personal information to them takes place. Motorola Solutions will communicate any substantial changes to the list of Group Members on an annual basis. Otherwise, an up-to-date list of Group Members will be provided to the Information Commissioner's Office where required.

The Rules became effective on 1 January 2021. The Rules apply to all personal information processed by Motorola Solutions or its service providers under these Rules on or after that date

and the Rules will take precedence over any other policies or procedures within Motorola Solutions relating to the collection and use of personal information.

Government Requests for Disclosure of Personal Information

If a Group Member receives a legally binding request for disclosure of personal information by a law enforcement authority or state security body which is subject to the Rules, it must comply with the Government Data Request Procedure set out in Appendix 7.

Important terms used in these Rules

For the purposes of these Rules:

- the term **applicable data protection laws** includes the data protection laws in force in the territory from which a Group Member initially transfers personal information under these Rules. Where a UK Group Member transfers personal information under these Rules to a non-UK Group Member, the term applicable data protection laws shall include the UK data protection laws;
- the term **controller** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal information. For example, Motorola Solutions is a controller of its HR records and CRM records;
- the term **GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679);
- the term **Group Member** means the members of Motorola Solutions' group of companies listed in Appendix 1;
- the term **personal information** means any information relating to an identified or identifiable natural person. An identifiable natural personal is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that nature personal;
- the term **processing** means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- the term **processor** means a natural or legal person which processes personal information on behalf of a controller (for example, a third party service provider that is processing personal information in order to provide a service to Motorola Solutions);
- the term **special category personal data** means information that relates to an individual's 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, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about an individual's criminal offenses or convictions, as well as any other information deemed sensitive under applicable data protection laws;
- The term **staff** refers to all employees, new hires, individual contractors and consultants, and temporary staff engaged by any Motorola Solutions Group Member. All staff must comply with these rules; and
- The term **UK data protection laws** means the GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018.