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.

Motorola Solutions

Binding Corporate Rules:

Appendix 1 - List of Motorola Solutions Group Members

Motorola Solutions Group Members

Beginning **February 14, 2022** the table below lists the Motorola Solutions UK group members which are bound by Motorola Solutions' "Binding Corporate Rules-Controller" (BCR-C).

Name	Country
Motorola Solutions UK Limited	United Kingdom
Airwave Solutions Limited	United Kingdom
Avigilon UK Limited	United Kingdom
Ava Security Limited	United Kingdom
Ava Video Security Limited	United Kingdom
Calipsa Limited	United Kingdom
Barrett Europe Limited	United Kingdom

Motorola Solutions Group Members

Beginning **February 14, 2022** the table below lists the Motorola Solutions EEA group members which are bound by Motorola Solutions' "Binding Corporate Rules-Controller" (BCR-C).

Name	Country
Motorola Solutions Austria Gmbh	Austria
Motorola Solutions Belgium SA	Belgium
Motorola Solutions Czech Republic s.r.o.	Czech Republic
Motorola Solutions Danmark A/S	Denmark
Dansk Beredskabskommunikation A/S	Denmark
Motorola Solutions France SAS	France
Motorola Solutions Germany GmbH	Germany
Airwave Solutions Deutschland GmbH	Germany
Motorola Solutions Hellas A.E.	Greece
Tetra Ireland Communications Limited	Ireland
Motorola Solutions Italia SRL	Italy
Videotec S.R.L.	Italy
Motorola Solutions Netherlands BV	Netherlands
Motorola Solutions Norway AS	Norway
Motorola Solutions Polska S.p z.o.o.	Poland
Motorola Solutions Systems Polska S.p z.o.o.	Poland
Motorola Solutions Portugal Lda	Portugal
Motorola Solutions Romania SRL	Romania
Motorola Solutions Espana SA	Spain
Motorola Solutions Sweden AB	Sweden

Motorola Solutions

UK Binding Corporate Rules:

Appendix 2 - Fair Information Disclosures

February 14, 2022

1. Background

1.1 Motorola Solutions' UK Binding Corporate Rules (Controller Policy) provides a framework for the transfer of personal information between Motorola Solutions Group Members.

1.2 This Fair Information Disclosure document sets out the transparency information that Motorola Solutions must provide to individuals when processing their personal information.

2. Information to be provided where Motorola Solutions collects personal information directly from individuals

2.1 When Motorola Solutions collects personal information directly from individuals, it must provide the following transparency information:

(a) the identity and contact details of the data controller and, where applicable, of its representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal information are intended as well as the legal basis for the processing;

(d) where the processing is based on Motorola Solutions' or a third party's legitimate interests, the legitimate interests pursued by Motorola Solutions or by the third party;

(e) the recipients or categories of recipients of the personal information, if any;

(f) where applicable, the fact that a group member in the UK intends to transfer personal information to a third country or international organization outside of the UK, and the measures that the group member will take to ensure the personal information remains protected in accordance with applicable data protection laws and how to obtain a copy of such measures.

2.2 In addition to the information above, Motorola Solutions shall also provide individuals with the following further information necessary to ensure fair and transparent processing, at the time of collection:

(a) the period for which the personal information will be stored, or if that is not possible, the criteria used to determine that period;

(b) information about the individuals' rights to request access to, rectify or erase their personal information, as well as the right to restrict or object to the processing, and the right to data portability;

(c) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with the Information Commissioner's Office;

(e) whether the provision of personal information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal information and of the possible consequences of failure to provide such information;

(f) the existence of automated decision-making, including profiling, and, where such decisions may have a legal effect or significantly affect the individuals whose personal information are collected, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for those individuals.

2.3 The transparency information described in this paragraph must be provided at the time that Motorola Solutions obtains the personal information from the individual.

3. Information to be provided where Motorola Solutions collects personal information about individuals from a third party source

3.1 When Motorola Solutions collects personal information from a third party source (that is, someone other than the individual him- or herself), it must provide the following transparency information:

(a) the information described in paragraphs 2.1 and 2.2 above;

(b) the categories of personal information that are being processed; and

(c) details of the third party source from which Motorola Solutions obtained the personal information including, if applicable, identifying whether the personal information came from publicly accessible sources.

3.2 The transparency information described in this paragraph must be provided within a reasonable period after Motorola Solutions obtains the personal information and, at the latest, within one month, having regard to the specific circumstances in which the personal information are processed. In addition:

(a) if the personal information are to be used for communication with the individual, the transparency information described in this paragraph must be provided at the latest at the time of the first communication to that individual; and

(b) if a disclosure of the personal information to another recipient is envisaged, the transparency information described in this paragraph must be provided at the latest when the personal information are first disclosed.

4. Derogations from providing transparency disclosures

4.1 The requirements to provide transparency information as described in this Fair Information Disclosures document shall not apply where and insofar as:

(a) the individual already has the information;

(b) the provision of such information provides impossible or would involve a disproportionate effort, and Motorola Solutions takes appropriate measures, consistent with the requirements of applicable data protection laws, to protect the individual's rights and freedoms and legitimate interests, including by making the transparency information publicly available;

(c) obtaining or disclosure is expressly laid down by applicable laws to which Motorola Solutions is subject and these laws provide appropriate measures to protect the individual's legitimate interests;

(d) where the personal information must remain confidential subject to an obligation of professional secrecy regulated by applicable laws to which Motorola Solutions is subject, including a statutory obligation of secrecy.

Motorola Solutions

UK Binding Corporate Rules:

Appendix 3 -
Data Subject Rights Procedure

1. Background

1.1 Motorola Solutions' UK Binding Corporate Rules (Controller Policy) (**"the Rules"**) safeguard personal information transferred between the Motorola Solutions Group Members.

1.2 Individuals whose personal information are processed by Motorola Solutions under the Rules have certain data protection rights, which they may exercise by making a request to the controller of their information (whether the controller is Motorola Solutions) (a **"Data Protection Rights Request"**).

1.3 This UK Binding Corporate Rules: Data Protection Rights Procedure ("Procedure") describes how Motorola Solutions will respond to any Data Protection Rights Requests it receives from individuals whose personal information are processed and transferred under the Rules.

2. Individual's data protection rights

2.1. Motorola Solutions must assist individuals to exercise the following data protection rights, consistent with the requirements of applicable data protection laws:

(a) **The right of access:** This is the right for individuals to obtain confirmation whether a controller processes personal information about them and, if so, to be provided with details of that personal information and access to it. This process for handling this type of request is described further in paragraph 4 below;

(b) **The right to rectification:** This is the right for individuals to require a controller to rectify without undue delay any inaccurate personal information a controller may be processing about them. The process for handling this type of request is described further in paragraph 5 below.

(c) **The right to erasure:** This is the right for individuals to require a controller to erase personal information about them on certain grounds – for example, where the personal information is no longer necessary to fulfill the purposes for which it was collected. The process for handling this type of request is described further in paragraph 5 below.

(d) **The right to restriction:** This is the right for individuals to require a controller to restrict processing of personal information about them on certain grounds. The process for handling this type of request is described further in paragraph 5 below.

(e) **The right to object:** This is the right for individuals to object, on grounds relating to their particular situation, to a controller's processing of personal information about them, if certain grounds apply. The process for handling this type of request is described further in paragraph 5 below.

(f) **The right to data portability:** This is the right for individuals to receive personal information concerning them from a controller in a structured, commonly used and machine-readable format and to transmit that information to another controller, if certain grounds apply. The process for handling this type of request is described further in paragraph 6 below.

(g) **The right not to be subject to automated decision making:** This is the right for individuals not to be subject to a decision based solely on automated processing, including profiling as described further in paragraph 7 below.

3. Responsibility to respond to a Data Protection Rights Request

3.1 *Overview*

3.1.1 The controller of an individual's personal information is primarily responsible for responding to a Data Protection Rights Request and for helping the individual concerned to exercise his or her rights under applicable data protection laws.

3.1.2 As such, when an individual contacts Motorola Solutions to make any Data Protection Rights Request then where Motorola Solutions is the controller of that individual's personal information under the Controller Policy, it must help the individual to exercise his or her data protection rights directly in accordance with this Procedure.

3.2 *Assessing responsibility to respond to a Data Protection Rights Request*

3.2.1 If a group member receives a Data Protection Rights Request from an individual, it must pass the request to the Privacy team using privacy1@motorolasolutions.com immediately

upon receipt indicating the date on which it was received together with any other information which may assist the Privacy team to deal with the request.

3.2.2 The Privacy team will make an initial assessment of the request as follows:

(a) the Privacy team will determine whether Motorola Solutions is a controller or processor of the personal information that is the subject of the request;

(b) where Privacy team determines that Motorola Solutions is a controller of the personal information, it will then determine whether the request has been made validly under applicable data protection laws (in accordance with section 3.3 below), whether an exemption applies (in accordance with section 3.4 below) and respond to the request (in accordance with section 3.5 below); and

(c) where Privacy team determines that Motorola Solutions is a processor of the personal information on behalf of a Customer, it shall pass the request promptly to the relevant Customer in accordance with its contract terms with that Customer and will not respond to the request directly unless authorized to do so by the Customer.

3.3 *Assessing the validity of a Data Protection Rights Request*

3.3.1 If Privacy team determines that Motorola Solutions is the controller of the personal information that is the subject of the request, it will contact the individual promptly in writing to confirm receipt of the Data Protection Rights Request.

3.3.2 A Data Protection Rights Request must generally be made in writing, which can include email, unless applicable data protection laws allow a request to be made orally. A Data Protection Rights Request does not have to be official or mention data protection law to qualify as a valid request.

3.3.3 If Motorola Solutions has reasonable doubts concerning the identity of the individual making a request, it may request such additional information as is necessary to confirm the identity of the individual making the request. Motorola Solutions may also request any further information which is necessary to action the individual's request.

3.4 *Exemptions to a Data Protection Rights Request*

3.4.1 Motorola Solutions will not refuse to act on Data Protection Rights Request unless it can demonstrate that an exemption applies under applicable data protection laws.

3.4.2 Motorola Solutions may be exempt under applicable data protection laws from fulfilling the Data Protection Rights Request if it can demonstrate that the individual has made a manifestly unfounded or excessive request (in particular, because of the repetitive character of the request).

3.4.3 If Motorola Solutions decides not to take action on the Data Protection Rights Request, Motorola Solutions will inform the individual without delay and at the latest within one (1) month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Information Commissioner's Office and seeking a judicial remedy.

3.5 *Responding to a Data Protection Rights Request*

3.5.1 Where Motorola Solutions is the controller of the personal information that is the subject of the Data Protection Rights Request, and Motorola Solutions has already confirmed the identity of the requestor and has sufficient information to enable it to fulfil the request (and no exemption applies under applicable data protection laws), then Motorola Solutions shall deal with the Data Protection Rights Request in accordance with paragraph 4, 5 or 6 below (as appropriate).

3.5.2 Motorola Solutions will respond to a Data Protection Rights Request without undue delay and in no case later than one (1) month of receipt of that request. This one (1) month period may be extended by two (2) further months where necessary, if the request is complex or due to the number of requests that have been made.

4. Requests for access to personal information

4.1 *Overview*

4.1.1 An individual may require a Controller to provide the following information concerning processing of his or her personal information:

(a) confirmation as to whether the controller holds and is processing personal information about that individual;

(b) if so, a description of the purposes of the processing, the categories of personal information concerned, the recipients or categories of recipients to whom the information is, or may be, disclosed, the envisaged period(s) (or the criteria used for determining those period(s)) for which the personal information will be stored;

(c) information about the individual's right to request rectification or erasure of his or her personal information or to restrict or object to its processing;

(d) information about the individual's right to lodge a complaint with the Information Commissioner's Office;

(e) information about the source of the personal information if it was not collected from the individual;

(f) details about whether the personal information is subject to automated decision-making (including automated decision-making based on profiling); and

(g) where personal information is transferred outside the UK, the appropriate safeguards that Motorola Solutions has put in place relating to such transfers in accordance with applicable data protection laws.

4.1.2 An individual is also entitled to request a copy of his or her personal information from the controller. Where an individual makes such a request, the controller must provide that personal information to the individual in intelligible form.

4.2 *Process for responding to access requests from individuals*

4.2.1 If Motorola Solutions receives an access request from an individual, this must be passed to the Privacy team at privacy1@motorolasolutions.com immediately to make an initial assessment of responsibility consistent with the requirements of paragraph 3.2 above.

4.2.2 Where Motorola Solutions determines it is the controller of the personal information and responsible for responding to the individual directly (and that no exemption to the right of access applies under applicable data protection laws), Data Protection Officer will arrange a search of all relevant electronic and paper filing systems.

4.2.3 The Privacy team may refer any complex cases to the Data Protection Officer and / or VP of Data Protection for advice, particularly where the request concerns information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.

4.2.4 The personal information that must be disclosed to the individual will be collated by the Privacy team into a readily understandable format. A covering letter will be prepared by the Privacy team which includes all information required to be provided in response to an individual's access request (including the information described in paragraph 4.1.1).

4.3 *Exemptions to the right of access*

4.3.1 A valid request may be refused on the following grounds:

(a) If the refusal to provide the information is consistent with applicable data protection law (for example, where a UK group member transfers personal information under the Controller Policy, if the refusal to provide the information is consistent with UK data protection laws);

(b) where the personal information is held by Motorola Solutions in non-automated form that is not or will not become part of a filing system;

(c) the personal information does not originate from the UK, has not been processed by any UK group member, and the provision of the personal information requires Motorola Solutions to use disproportionate effort.

4.3.2 The Privacy team will assess each request individually to determine whether any of the above-mentioned exemptions applies. A group member must never apply an exemption unless this has been discussed and agreed with Data Protection Officer.

5. Requests to correct, update or erase personal information, or to restrict or cease processing personal information

5.1.1 If Motorola Solutions receives a request to correct, update or erase personal information, or to restrict or cease processing of an individual's personal information, this must be passed to the Privacy team at privacy1@motorolasolutions.com immediately to make an initial assessment of responsibility consistent with the requirements of paragraph 3.2 above.

5.2 Once an initial assessment of responsibility has been made then where Motorola Solutions is the controller of that personal information, the request must be notified to the Privacy team and Data Protection Officer promptly for it to consider and deal with as appropriate in accordance with applicable data protection laws.

5.3 When Motorola Solutions must rectify or erase personal information in its capacity as controller, Motorola Solutions will notify other group members and any processor to whom the personal information has been disclosed so that they can also update their records accordingly.

5.4 If Motorola Solutions acting as controller has made the personal information public, and is obliged to erase the personal data pursuant to a Data Protection Rights Request, it must take reasonable steps, including technical measures (taking account of available technology and the cost of implementation), to inform controllers which are processing the personal information that the individual has requested the erasure by such controllers of any links to, or copy or replication of, the personal information.

6. Requests for data portability

6.1 If an individual makes a Data Protection Rights Request to Motorola Solutions acting as controller to receive the personal information that he or she has provided to Motorola Solutions in a structured, commonly used and machine-readable format and/or to transmit directly such information to another controller (where technically feasible), Motorola Solutions' Privacy, Information Security and / or business teams will consider and deal with the request appropriately in accordance with applicable data protection laws insofar as the processing is based on that individual's consent or on the performance of, or steps taken at the request of the individual prior to entry into, a contract.

7. Requests regarding automated decision making

7.1 The right not to be subject to automated decision making is the right for individuals not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless it is: a) necessary for entering into or performance of a contract between the individual and the controller, b) authorized by Union or Member State law to which the controller is subject and

which also lays down suitable measures to safeguard the individual's rights and freedoms and legitimate interests, or c) the individual has given their explicit consent. If an individual makes a Data Protection Rights Request to Motorola Solutions acting as controller not to be subject to automated decision making (including profiling), Motorola Solutions' Privacy team will consider and deal with the request appropriately in accordance with applicable data protection laws. This may include, if requested, provision of information about the logic involved in the decision.

8. Questions about this Data Protection Rights Procedure

8.1 All queries relating to this Procedure are to be addressed to the Motorola Solutions Data Protection Office or at privacy1@motorolasolutions.com.

Motorola Solutions

UK Binding Corporate Rules:

Appendix 4 - Complaint Handling Procedure

February 14, 2022

1. Background

1.1 Motorola Solutions' UK Binding Corporate Rules (Controller Policy) ("the Rules") safeguard personal information transferred between the Motorola Solutions Group Members.

1.2 This Complaint Handling Procedure describes how complaints brought by an individual whose personal information is processed by Motorola Solutions under the Rules must be addressed and resolved.

1.3 This procedure will be made available to individuals whose personal information is processed by Motorola Solutions under the Rules.

2. How individuals can bring complaints

2.1 Any individuals may raise a data protection question, concern or complaint (whether related to the Rules or not) by e-mailing Motorola Solutions' Privacy Team at privacy1@motorolasolutions.com.

3. Complaints where Motorola Solutions is a controller

3.1 *Who handles complaints?*

3.1.1 The Privacy Team will handle all questions, concerns, or complaints in respect of personal information for which Motorola Solutions is a controller, including questions, concerns or complaints arising under the Rules. The Privacy Team will liaise with colleagues from relevant business and support units as necessary to address and resolve such questions, concerns and complaints.

3.2 *What is the response time?*

3.2.1 The Privacy Team will acknowledge receipt of a question, concern or complaint to the individual concerned without undue delay, investigating and making a substantive response within one (1) month.

3.2.2 If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Privacy Team will advise the individual accordingly and provide a reasonable estimate (not exceeding two (2) months) of the timescale within which a substantive response will be provided.

3.3 *What happens if an individual disputes a finding?*

3.3.1 If the individual notifies the Privacy Team that it disputes any aspect of the response finding, the Privacy Team will refer the matter to the Data Protection Officer / VP Data Protection. The Data Protection Officer / VP Data Protection will review the case and advise the individual of his or her decision either to accept the original finding or to substitute a new finding. The Data Protection Officer / VP Data Protection will respond to the complainant within one (1) month from being notified of the escalation of the dispute.

3.3.2 As part of its review, the Data Protection Officer / VP Data Protection may arrange to meet the parties to the dispute in an attempt to resolve it. If, due to the complexity of the dispute, a substantive response cannot be given within one (1) month of its escalation, the Data Protection Officer / VP Data Protection will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will not exceed two (2) months from the date the dispute was escalated.

3.3.3 If the complaint is upheld, the Data Protection Officer / VP Data Protection will arrange for any necessary steps to be taken as a consequence.

4. Right to complain to a the Information Commissioner's Office and to commence proceedings

4.1 *Overview*

4.1.1 Where individuals' personal information:

(a) are processed in the UK by a Group Member acting as a controller and/or transferred to a Group Member located outside the UK under the Controller Policy; or

(b) are processed in the UK by a Group Member acting as a processor and/or transferred to a Group Member located outside the UK under the Controller Policy;

then those individuals have certain additional rights to pursue effective remedies for their complaints, as described below.

4.1.2 The individuals described above have the right to complain to the Information Commissioner's Office (in accordance with paragraph 5.2) and/or to commence proceedings in a court of competent jurisdiction (in accordance with paragraph 5.3), whether or not they have first complained directly to Motorola Solutions under this Complaints Handling Procedure.

4.1.3 Motorola Solutions accepts that complaints and claims made pursuant to paragraphs 4.2 and 4.3 may be lodged by a non-for-profit body, organization or association acting on behalf of the individuals concerned.

4.2 *Complaint to the Information Commissioner's Office*

4.2.1 If an individual wishes to complain about Motorola Solutions' processing of his or her personal information to the Information Commissioner's Office, on the basis that a UK Group Member has processed personal information in breach of the Rules or in breach of applicable data protection laws, he or she may complain about that UK Group Member to the Information Commissioner's Office:

(a) of his or her habitual residence;

(b) of his or her place of work; or

(c) where the alleged infringement occurred.

4.2.2 If an individual wishes to complain about Motorola Solutions' processing of his or her personal information to the Information Commissioner's Office, on the basis

that a non-UK Group Member has processed personal information in breach of the Rules or in breach of applicable data protection laws, then will submit to the jurisdiction of the competent Information Commissioner's Office (determined in accordance with paragraph 5.2.1) in place of that non-UK Group Member, as if the alleged breach had been caused by Motorola Solutions UK Limited.

4.3 *Proceedings before a national court*

4.3.1 If an individual wishes to commence court proceedings against Motorola Solutions, on the basis that a UK Group Member has processed personal information in breach of the Rules or in breach of applicable data protection laws, then he or she may commence proceedings against that UK Group Member in the UK:

(a) in which that UK Group Member is established; or

(b) of his or her habitual residence.

4.3.2 If an individual wishes to commence court proceedings against Motorola Solutions, on the basis that a non-UK Group Member has processed personal information in breach of the Rules or in breach of applicable data protection laws, then Motorola Solutions UK Limited will submit to the jurisdiction of the competent court (determined in accordance with paragraph 5.3.1) in place of that non-UK Group Member, as if the alleged breach had been caused by Motorola Solutions UK Limited.

Motorola Solutions

UK Binding Corporate Rules:

Appendix 5 - Cooperation Procedure

1. Background

1.1 Motorola Solutions' UK Binding Corporate Rules: Cooperation Procedure sets out the way in which Motorola Solutions will cooperate with the Information Commissioner's Office in relation to the Motorola Solutions UK Binding Corporate Rules (Controller Policy) ("the Rules").

2. Cooperation Procedure

2.1 Where required, Motorola Solutions will make the necessary personnel available for dialogue with the Information Commissioner's Office in relation to the Rules.

2.2 Motorola Solutions will:

(a) comply with any advice or decision of the Information Commissioner's Office on any data protection law issues that may affect the Rules subject to any effective judicial remedy and due process which may apply and which Motorola Solutions chooses to exercise including any right of appeal; and

(b) review, consider and (as appropriate) implement any guidance published by the Information Commissioner's Office in connection with Binding Corporate Rules for Processors and Binding Corporate Rules for Controllers.

2.3 Motorola Solutions will provide upon request copies of the results of any audit it conducts of the Rules to the Information Commissioner's Office, who will treat the audit results in accordance with any confidentiality obligations applicable to the Information Commissioner's Office under applicable data protection law.

2.4 Motorola Solutions agrees that the Information Commissioner's Office may audit any Group Member who processes personal information as a controller for compliance with the Rules.

2.5 Motorola Solutions agrees to comply with the advice of and abide by a formal decision of the Information Commissioner's Office on any issues relating to the interpretation and application of the Rules subject to any effective judicial remedy and

due process which may apply and which Motorola Solutions chooses to exercise including any right of appeal.

2.6 In the event of a conflict between the provisions of this Appendix 5 (Cooperation Procedure) and the applicable data protection law of a non-UK country, the "Relationship between national laws and the Rules" provisions of the Rules shall apply.

Motorola Solutions

UK Binding Corporate Rules:

Appendix 6 - Privacy Training Requirements

February 14, 2022

1. Background

1.1 Motorola Solutions' UK Binding Corporate Rules (Controller Policy) (**"the Rules"**) provides a framework for the transfer of personal information between Motorola Solutions Group Members.

1.2 The document sets out the requirements for Motorola Solutions to train its staff members on the requirements of the Rules.

1.3 Motorola Solutions must train staff members (including new hires, temporary staff and individual contractors whose roles bring them into contact with personal information) on the basic principles of data protection, confidentiality and information security awareness. This must include training on UK data protection laws. Staff members who have permanent or regular access to personal information and who are involved in the processing of personal information or in the development of tools to process personal information must receive additional, tailored training on the Rules and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis.

2. Responsibility for the Privacy Training Program

2.1 Motorola Solutions' Privacy Team has overall responsibility for privacy training at Motorola Solutions, with input with colleagues from other functional areas including Information Security, HR and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Rules and that it is appropriate for individuals who have permanent or regular access to personal information, who are involved in the processing of personal information or in the development of tools to process personal information.

2.2 Motorola Solutions' senior management is committed to the delivery of data protection training courses, and will ensure that staff are required to participate, and given appropriate time to attend such courses. Course attendance must be recorded and monitored via regular reviews of the training process. These reviews are facilitated by Motorola Solutions' Ethics & Compliance Team and/or independent third party auditors.

2.3 If these training reviews reveal persistent non-completion, this will be escalated to VP, Ethics & Compliance for action. Such action may include escalation of non-completion to

appropriate managers within Motorola Solutions who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participate in such training.

3. Delivery of the training courses

3.1 Motorola Solutions will deliver mandatory electronic training courses, supplemented by face to face training for staff members. The courses are designed to be both informative and user-friendly, generating interest in the topics covered. All Motorola Solutions staff members must complete data protection training (including training on the Rules):

(a) as part of their induction program;

(b) as part of a regular refresher training at least once every 2 years ;

(c) as and when necessary to stay aware of changes in the law; and

(d) as and when necessary to address any compliance issues arising from time to time.

3.2 Certain staff members must receive supplemental specialist training, in particular staff members who work in HR, Marketing, Sales, Products & Services, Procurement and Customer Support or whose business activities include processing special category personal data. Specialist training shall be delivered as additional modules to the basic training package, and will be tailored as necessary to the course participants.

4. Training on data protection

4.1 Motorola Solutions' training on data protection and the Rules will cover the following main areas:

4.1.1 Background and rationale:

(a) What is data protection law?

(b) What are key data protection terminology and concepts?

(c) What are the data protection principles?

(d) How does data protection law affect Motorola Solutions internationally?

(e) What are Motorola Solutions' BCR Rules?

4.1.2 The Rules:

(a) An explanation of the Rules

(b) The scope of the Rules

(c) The requirements of the Rules

(d) Practical examples of how and when the Rules apply

(e) The rights that the Rules give to individuals

(f) The privacy implications arising from processing personal information for clients

4.1.3 Where relevant to a staff member's role, training will cover the following procedures under the Rules:

(a) Data Subject Rights Procedure

(b) Cooperation Procedure

(c) Complaint Handling Procedure

(d) Government Data Request Procedure

Motorola Solutions

UK Binding Corporate Rules:

Appendix 7 - Government Data Request Procedure

February 14, 2022

1. Background

1.1 Motorola Solutions' UK Binding Corporate Rules: Government Data Request Procedure sets out Motorola Solutions' procedure for responding to a request received from a law enforcement authority or state security body (together the **"Requesting Authority"**) to disclose personal information processed by Motorola Solutions (hereafter **"Data Disclosure Request"**).

1.2 Where Motorola Solutions receives a Data Disclosure Request, it will handle that Data Disclosure Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal information than is required by this Procedure, Motorola Solutions will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Disclosure Requests

2.1 As a general principle, Motorola Solutions does not disclose personal information in response to a Data Disclosure Request unless either:

(a) it is under a compelling legal obligation to make such disclosure; or

(b) taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

2.2 For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, Motorola Solutions will notify and cooperate with the Information Commissioner's Office if it is the competent Supervisory Authority (and, where it processes the requested personal information on behalf of a Customer, the Customer) in order to address the Data Disclosure Request.

3. Handling of a Data Disclosure Request

3.1 *Receipt of a Data Disclosure Request*

3.1.1 If a Motorola Solutions Group Member receives a Data Disclosure Request, the recipient of the request must pass it to Motorola Solutions' Data Protection Officer, immediately

upon receipt, indicating the date on which it was received together with any other information which may assist Motorola Solutions' Data Protection Office to deal with the request.

3.1.2 The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Disclosure Request. Any Data Disclosure Request, howsoever made, must be notified to Data Protection Office for review.

3.2 *Initial steps*

3.2.1 Motorola Solutions' Data Protection Office will carefully review each and every Data Disclosure Request on a case-by-case basis. Motorola Solutions' Data Protection Office will liaise with the legal department as appropriate to deal with the request to determine the nature, context, purposes, scope and urgency of the Data Disclosure Request, as well as its validity under applicable laws, in order to identify whether action may be needed to challenge the Data Disclosure Request.

4. Notice of a Data Disclosure Request

4.1 *Notice to the Information Commissioner's Office*

4.1.1 Motorola Solutions will put the request on hold in order to notify and consult with the Information Commissioner’s Office where it is the competent Supervisory Authority, unless legally prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation) or where an imminent risk of serious harm exists that prohibits prior notification. Such notification to the Information Commissioner's Office will include, information about the data requested, the requesting body, and the legal basis for the disclosure. Where Motorola Solutions is not reasonably able to notify the Information Commissioner's Office of a Data Disclosure Request due to imminent risk of serious harm, provided Motorola Solutions is not legally prohibited from doing so, Motorola Solutions will notify the Information Commissioner's Office when it is reasonably able to do so.

4.1.2 Where Motorola Solutions is prohibited from notifying the Information Commissioner's office and suspending the request, Motorola Solutions will use its best efforts (taking into account the nature, context, purposes, scope and urgency of the request) to inform the Requesting Authority about its obligations under applicable data protection law and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that Motorola Solutions can consult with the Information

Commissioner's Office, which may also, in appropriate circumstances, include seeking a court order to this effect. Motorola Solutions will maintain a written record of the efforts it takes.

5. Transparency reports

5.1 If, despite having used its best efforts, Motorola Solutions is not in a position to notify the Information Commissioner's Office, Motorola Solutions commits to preparing an annual report (a **"Transparency Report"**), which reflects to the extent permitted by applicable laws, the number and type of Data Disclosure Requests it has received for the preceding year and the Requesting Authorities who made those requests. Motorola Solutions shall provide this report to the Information Commissioner's Office once each year.

6. Bulk transfers

6.1 In no event will any Group Member transfer personal information to a Requesting Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

Motorola Solutions

UK Binding Corporate Rules:

Appendix 8 –

Material Scope of the Controller Policy

February 14, 2022

1. Background

1.1 The “UK Binding Corporate Rules: Controller Policy” (the "**Controller Policy**") provides a framework for the transfer of personal information between Group Members.

1.2 This document sets out the material scope of the Controller Policy. It specifies the data transfers or set of transfers, including the nature and categories of personal information, the type of processing and its purposes, the types of individuals affected, and the identification of the third country or countries.

2. Human Resources Data

Who transfers the personal information described in this section?	Every Group Member inside of the UK may transfer the personal information that they control described in this section to every other Group Member inside and outside of the UK. Every Group Member outside of the UK may also transfer the personal information that they control described in this section to every Group Member inside and outside of the the UK.
Who receives this personal information?	Every Group Member outside of the UK may receive the personal information described in this section which is sent to them by other Group Members inside and outside of the UK. Every Group Member inside of the UK may also receive the personal information described in this section which is sent to them by other Group Members inside and outside of the UK.

What categories of personal information are transferred?	Group Members collect and transfer Special Category Personal Information only in connection with valid employment purposes. Such collection and transfer will only concern limited Sensitive Personal Information, for example, health-related information for the purpose of managing employee absences, disabilities in order to provide access to our premises, and diversity information (e.g. race and ethnic origin, religion, sexual orientation and disabilities) for equal opportunities monitoring. Group Members may also collect and transfer background checking information on certain prospective employees, but only where and to the extent permitted by law.
Who are the types of individuals whose personal information are transferred?	Past and current staff 1. Individual consultants 2. Independent contractors 3. Temporary staff 4. Job applicants
Why is this personal information transferred and how will it be used?	The management of employment-related activities including but not limited to: ● recruitment; ● entering, performing and changing employment or service contracts; ● contacting staff or others on their behalf; ● payroll and benefits administration; ● supporting and managing staff work and performance and any health concerns;

	• changing or ending staff working arrangements; • physical and system security; • providing references; • providing staff information to third parties in connection with transactions that are contemplated or carried out; • monitoring of diversity and equal opportunities; • monitoring and investigating compliance with legal obligations, internal policies and rules both generally and specifically, including implementing and operating a whistleblowing hotline; • disputes and legal proceedings; • day-to-day business operations, including marketing and customer/client relations; and • maintaining appropriate business records during and after employment or engagement.
Where is this personal information processed?	The personal information described in this section may be processed in every territory where Group members or their processors are located.

3. Customer Relationship Management Data

Who transfers the personal information described in this section?	Every Group Member inside of the UK may transfer the personal information that they control described in this section to every other Group Member inside and outside of the UK. Every Group Member outside of the UK may also transfer the personal information that they control described in this section to every Group Member inside and outside of the UK.
Who receives this personal information?	Every Group Member outside of the UK may receive the personal information described in this section which is sent to them by other Group Members inside and outside of the UK. Every Group Member inside of the UK may also receive the personal information described in this section which is sent to them by other Group Members inside and outside of the UK.
What categories of personal information are transferred?	• Contact details: postal address, billing address, delivery address, phone number (fixed and mobile), email address, fax number and other personal details provided by customers of the Group Member and visitors to the Group Members' websites and other digital properties. • Professional details: job title, affiliated organization, data relating to business projects.

	• Financial data: bank account number, bank details, payment card details. • Order data: purchasing history, return history, cancellation history. • IT related data: IP addresses of visitors to the Group Members' websites and other digital properties, online navigation data, browser type, language preferences, pixel data, cookies data, web beacon data. • Social security numbers or equivalent national identification numbers and date of birth. • Information on sweepstakes or contests you customers enter. • Survey and questionnaire responses. ○ • Blog posts and social media posts. • Email correspondence. • Information available from online directories and databases.
What categories of sensitive personal information (if any) are transferred?	None.
Who are the types of individuals whose personal information are transferred?	Representatives of business customers.
Why is this personal information transferred and how will it be used?	The management and administration of customer services including but not limited to:

	• the administration of orders and accounts; • providing products and services; • product management; • business development; • performance analysis including volume / frequency of orders / deliveries; • marketing, advertising and public relations in connection with Group Members' business activities, goods or services; • customer relationship management including satisfaction surveys, customer claims and after sales service; and • the conduct of Group Members' business activities.
Where is this personal information processed?	The personal information described in this section may be processed in every territory where Group members or their processors are located.

4. Supply chain management data

Who transfers the personal information described in this section?	Every Group Member inside of the UK may transfer the personal information that they control described in this section to every other Group Member inside and outside of the UK.

	Every Group Member outside of the UK may also transfer the personal information that they control described in this section to every Group Member inside and outside of the UK.
Who receives this personal information?	Every Group Member outside of the UK may receive the personal information described in this section which is sent to them by other Group Members inside and outside of the UK. Every Group Member inside of the UK may also receive the personal information described in this section which is sent to them by other Group Members inside and outside of the UK.
What categories of personal information are transferred?	• Contact details: postal address, billing address, delivery address, phone number (fixed and mobile), email address, fax number and other personal details provided by customers of the Group Member and visitors to the Group Members' websites and other digital properties. • Professional details: job title, affiliated organization, data relating to business projects. • Financial data: bank account number, bank details, credit card details. • Order data: purchasing history, return history, cancellation history. • IT related data: IP addresses of visitors to the Group Members' websites and other digital properties, online navigation data,

	browser type, language preferences, pixel data, cookies data, web beacon data.
What categories of sensitive personal information (if any) are transferred?	None.
Who are the types of individuals whose personal information are transferred?	1. Individual contractors 2. Individual account managers 3. Staff or third party suppliers
Why is this personal information transferred and how will it be used?	The management and administration of supplier services including but not limited to: ● the management and administration of supplier accounts; ● the selection and vetting of suppliers; ● information gathering regarding suppliers; ● supplier relationship management; and ● statistics and data analytics.
Where is this personal information processed?	The personal information described in this section may be processed in every territory where Group members or their processors are located.