Motorola Solutions

Controller Binding Corporate Rules

1. Introduction

These Controller Binding Corporate Rules (**"Rules"**) explain how the Motorola Solutions group of companies ("Group Members") as controllers respect the privacy rights of its customers, staff, suppliers and other individuals whose personal information Group Members collect and use.

Due to the global nature of Group Members' businesses, Group Members may transfer personal information under these Rules to their ultimate parent company, Motorola Solutions, Inc. located in the United States, and to other Group Members in countries globally that may not provide a level of protection equivalent to the laws provided in the EEA . However, Group Members must ensure that the personal information of staff, customers, suppliers and other individuals whose personal information is collected and used by Group Members as a controller will only ever be treated in accordance with these Rules.

All Group Members and their staff must comply with these Rules as controllers when collecting or using any personal information. Group Members contractually commit to each other to comply with these Rules by signing a group agreement referred to as an 'intra-group agreement'. Group Members transfer personal information to other Group Members on a global basis as part of their regular business activities and the Rules will apply to all Group Members as controllers when such transfers 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 Group Members use it.

Group Members' management is fully committed to ensuring that Group Members and their staff comply with these Rules at all times. Group Members' 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.

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

2. 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 (whether an EEA Group Member or non-EEA Group Member) initially transfers personal information under these Rules. Where an EEA Group Member that is subject to the General Data Protection Regulation transfers personal information under these Rules to another Group Member, the term applicable data protection laws shall include the General Data Protection Regulation;
- 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, a Group Member is a controller of its HR records and CRM records;
- the term **EEA** as used in these Rules refers to the Member States of the European Economic Area – that is, the 27 Member States of the European Union plus Norway, Lichtenstein and Iceland;
- 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 Group Members);
- 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.
- The term **staff** refers to all employees, new hires, individual contractors and consultants, and temporary staff engaged by any Group Member. All staff must comply with these rules; and
- The term **Supervisory Authorities** means data protection authorities established in the EEA.

3. Scope of the Rules

These Rules apply whenever Group Members collect or use 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 another non-EEA country) to such other Group Member.

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

These Rules apply to all personal information that we process 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).

Each Group Member that is a controller for personal information shall be responsible for its own compliance with the Rules and shall be able to demonstrate its compliance including the records of processing referred to below.

4. Compliance with local law

Group Members 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, Group Members will process personal information in accordance with the Rules. Where applicable data protection laws grant a higher level of protection than the standards set out in the Rules we must comply with the standards of those applicable data protection laws.

5. Transparency and fairness

Group Members 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 Group Members 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.

6. Lawfulness of processing

We must always ensure that we have a lawful basis for processing personal information, consistent with the requirements of applicable data protection laws. These might include to enter into or perform a contract with you, to comply with legal obligations, to protect your vital interests, for public interest reasons or for our or a third party's legitimate interests. If an individual gives their consent to process their personal information that is also a valid lawful basis.

If we rely on an individual's consent to process personal information which is protected by applicable data protection law and transferred under these Rules, that consent must be given freely. To be freely given, the performance of a contract, including the provision of a service, must not be conditional on consent to processing of Personal Information being given if the processing is not necessary to perform the contract. It must also be specific, informed, intelligible and unambiguous, and given by way of a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity will not constitute consent. The consent must be clearly distinguishable from other matters and easily accessible. We must be able to demonstrate that consent was given. The individual must be able to withdraw their consent at any time as easily as when they gave their consent. Any such withdrawal of consent will not affect the lawfulness of processing based on consent before the consent was withdrawn.

7. Special category personal data

A Group Member must, in addition to having a general lawful basis for processing personal information, (as described above under section 6 'Lawfulness of processing') also have a second lawful basis if the personal information to be processed is special category personal data. The second lawful basis could be:

- To comply with the obligations of and exercise rights of a Group Member or individual under employment, social security and social protection laws;
- To protect the vital interests of an individual;
- Where the individual has themselves made the personal information public;
- To establish, exercise or defend legal claims;
- For reasons of substantial public interest;
- For preventative or occupational medicine purposes, for the assessment of the working capacity of employees, medical diagnoses, provision of health or social care or treatment or the management of health or social care systems and services;
- For reasons of public health such as protecting against serious cross-border threats; or
- For archiving in the public interest, scientific or historical research purposes or statistical purposes.

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

Group Members are permitted to process special category personal data with an individual's consent. When obtaining an individual's consent to use special category personal data, that consent must meet the criteria explained above for consent as the lawful basis for processing (see under section 6 above 'Lawful basis for processing') and be explicit.

8. Purpose limitation

Group Members shall collect and use personal information only for specified, explicit and legitimate purposes. Group Members 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. Processing of personal information in the public interest, scientific or historical research purposes or statistical purposes are examples of compatible purposes.

Group Members shall have a lawful basis for processing personal information which is protected under the General Data Protection Regulation for a different or new purpose.

See the section headed 'Lawfulness of processing' (section 6) and 'Special category personal data' (section 7) for a description of lawful basis that may be relied on by Group Members to process personal information.

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 regarding the relationship between individuals and the Group Members;
- the nature of the personal information, in particular whether such information may constitute special category personal data or whether the personal information relates to criminal convictions and offenses;
- the possible consequences of the intended further processing for the individuals concerned; and
- the existence of any appropriate safeguards, which may include encryption or pseudonymisation.

EEA law may permit processing of personal information for certain additional purposes and if so, Group Members may also process personal information for those additional purposes. These may include, for reasons of national security, defence, or public security, the prevention, investigation, detection or prosecution of criminal offices or execution of criminal penalties, to protect individuals and to safeguard against and prevent threats to public security and other important interests.

9. Data quality, proportionality and storage limitation

Group Members will ensure that personal information collected and used is:

- accurate and, where necessary, kept up-to-date;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

- processed in a manner that ensures appropriate security of the personal information (for more information on this please see under the heading "Security and Confidentiality of Data";
- 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 Group Members' Records Management Policy and relevant schedules, as amended from time to time.

Group Members must take every reasonable step to ensure that personal information that is inaccurate, taking into account the purposes for which they are processed, are erased or rectified without delay.

10. Transfers to third parties

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

For personal information initially subject to EEA data protection law when the personal information is transferred (or onward transferred) to third party data controllers or data processors outside of the EEA, this might be achieved as permitted by EEA data protection laws, including where the transfer of personal information:

- Is to a country or international organization where the European Commission 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 standard data protection clauses adopted by the European Commission or a Supervisory Authority and approved by the European Commission, European Data Protection Board and European Commission 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 EEA data protection laws. These permitted conditions include where the individual has given consent to the proposed transfer (having been informed of the possible risks of the transfer for the individual due to the absence of an adequacy decision and appropriate safeguards) or the transfer is necessary:

- To perform a contract between the individual and the controller or to implement pre-contractual measures at the individual's request;

- To conclude or perform a contract between the controller and another party which is in the interests of an individual;

- For important public interest reasons;

- To establish, exercise or defend legal claims; or

- To protect the vital interests of an individual where the individual is physically or legally incapable of giving consent.

A transfer of personal information is also permitted if it is from a publically available register which is intended to provide information to the public.

11. Publication of the Rules

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

12. Individual's data protection rights

Group Members must assist individuals whose personal information is collected or used in the EEA to exercise the following data protection rights (described in Appendix 3 "Data Protection Rights Procedure" in more detail), consistent with the requirements of applicable data protection laws:

- **The right of access:** This is a right for an individual to obtain confirmation whether a Group Member processes personal information about them and, if so, to be provided with access to, and a copy of, that personal information. Individuals may request to receive their personal information in a structured, commonly used and machine-readable format;

- **The right to rectification:** This is a right for an individual to obtain rectification without undue delay of inaccurate personal information a Group Member may process about him or her. Taking into account the purpose of Group Members' processing, it also includes the right for an individual to have incomplete personal information completed, including by means of a supplementary statement.
- **The right to erasure:** This is a right for an individual to require a Group Member to erase personal information about them on certain grounds, as described in the Data Protection Rights Procedure (see Appendix 3) – for example, where the personal information is no longer necessary to fulfill the purposes for which it was collected.
  If a Group Member has made the personal information public, then (taking account of available technology and the cost of implementation) the Group Member must also take reasonable steps, including technical measures, 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, that personal information.
- **The right to restriction:** This is a right for an individual to require a Group Member to restrict processing of personal information about them on certain grounds, as described in the Data Protection Rights Procedure (see Appendix 3).
- **The right to data portability:** This is a right for an individual to receive personal information concerning him or her from a Group Member in a structured, commonly used and machine-readable format and to transmit that information to another controller, if certain grounds apply as described in the Data Protection Rights Procedure (see Appendix 3). Where technically feasible, this may include direct transmission from a Group Member to another controller.
- **The right to object:** This is a right for an individual to object, at any time, on grounds relating to his or her particular situation, to processing of personal information about him or her, if certain grounds apply as described in the Data Protection Rights Procedure (see Appendix 3).

In addition, the relevant Group Member shall communicate any rectification or erasure of personal information or restriction of processing to each recipient to whom the personal information have been disclosed, unless this proves impossible or involves disproportionate effort. The Group Member must inform the individual about those recipients if the individual requests it.

13. How individuals can exercise their data protection rights

Where an individual wishes to exercise any of their data protection rights, Group Members must respect those rights in accordance with applicable law by following the Data Protection Rights Procedure (see Appendix 3).

Group Members' staff may exercise their data protection rights 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.

Group Members' customers, suppliers and other individuals may exercise their data protection rights by contacting Group Members 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 Group Members' Privacy & Data Security Compliance Committee.

14. The right to object to receiving marketing information

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

15. Automated individual decisions

Group Members 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 the General Data Protection Regulation, must be European Union or Member State 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.

Group Members 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.

16. Security and Confidentiality of Data

Group Members are committed to protecting the confidentiality, security and integrity of personal information.

To this end, Group Members 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, Group Members will deploy enhanced security measures whenever processing any special category personal data. Group Members will also ensure that their staff at all times adhere to Group Members' specific information security policies in place from time to time and process personal information only on instructions from Group Members and under a duty of confidence.

Group Members have 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

Group Members will ensure that providers of services to Group Members will also adopt appropriate security measures and will enter into contractual arrangements with the Group Member which require the service provider to:

- only act on the instructions of the Group Member 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 the Group Member 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 Supervisory Authorities, communication of personal data breaches to data subjects, data protection impact assessments and consultation with Supervisory Authorities 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 Group Member's 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:

- to notify competent data protection authorities, because the incident is likely to create a risk to the rights and freedoms of individuals affected by the incident; and
- to notify individuals affected by the incident, because the incident creates a high risk to their rights and freedoms.

The Data Protection Officer shall be responsible for ensuring that any such notifications, where necessary, are made in accordance with the requirements of, and timescales specified by, the General Data Protection Regulation.

The General Data Protection Regulation specifies that personal data related security incidents must be notified to the competent data protection authorities without undue delay and, where feasible, within 72 hours of becoming aware of the incident unless the incident is unlikely to result in a risk to the rights and freedoms of individuals.

If a required notification is not made within 72 hours it must be accompanied by reasons for the delay. The notification must describe the nature of the incident, including where possible, the categories and approximate numbers of individuals and personal data records affected. The notification must also provide the Data Protection Officer's name and contact details, the consequences of the incident and measures taken or to be taken, to address the incident and mitigate possible harm arising from it.

Where notification to affected individuals is also required, they must be notified without undue delay. Individuals must be notified of a personal data related security incident if there is likely to be a high risk to their rights and freedoms unless their personal information has been protected by measures such as encryption, the high risk of harm has been mitigated by subsequent measures or it would involve a disproportionate effort to make the notifications. If it would involve disproportionate effort, as an alternative a public communication or similar may be made. As for the notification to the competent data protection regulator, the notification should describe the nature of the incident and the Data Protection Officer's contact details, consequences of the incident and remedial and mitigation measures.

Group Members 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.

17. Training Program

Group Members 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.

18. Audit Program

Group Members 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 Privacy & Data Security Compliance Committee shall conduct periodic (at least annually) 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 Group Members' management.

Privacy Audits may cover all aspects of compliance with the Rules, including methods of ensuring that corrective actions will take place where appropriate.

The Privacy & Data Security Compliance Committee will determine the scope of an audit following a risk-based analysis, taking into account relevant criteria such as:

- areas of current regulatory focus;
- areas of specific or new risk for the business;
- areas with changes to the systems or processes used to safeguard information;
- use of innovative new tools, systems or technologies;
- areas where there have been previous audit findings or complaints;
- the period since the last review; and

- the nature and location of the personal information processed.

In addition, as part of its standards of internal control, the Group Members' 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, Inc.

Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Group Members will provide copies of the results of data protection audits of the Rules (including any related procedures and controls) to the competent Supervisory Authorities. The Privacy & Data Security Compliance Committee is responsible for liaising with the competent Supervisory Authorities for the purpose of providing the such copies.

The competent Supervisory Authorities may audit group members for compliance with the Rules (including any related procedures and controls) in accordance with Appendix 5 (Cooperation Procedure).

19. Data Protection Impact Assessments

Where required by applicable 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. Group Members 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 Personal Information is protected by the General Data Protection Regulation, Group Members must always conduct a DPIA whenever they intend to:

- perform a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning those individuals or similarly significantly affect them;
- process Special Category Personal Data on a large scale or process personal information relating to criminal convictions and offenses; or
- undertake a systematic monitoring of a publicly accessible area on a large scale.

Group Members must carry out regular reviews to assess if processing is still performed in accordance with their DPIAs, including at least when there is a change in the risk represented by their processing activities.

Where the DPIA indicates that the processing would still result in a high risk to individuals, Group Members will consult with local Supervisory Authorities where required by applicable data protection laws.

20. Records of Data Processing

Group Members must maintain a record of the processing activities that they conduct in accordance with applicable data protection laws. These records should be kept in writing (which may be in electronic form) and we must make these records available to competent Supervisory Authorities upon request.

Group Member records of processing must specify:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;

- a description of the categories of individuals whose personal information are processed and of the categories of personal information;
- the categories of recipients to whom the personal information have been or will be disclosed including recipients in third countries or international organizations;
- where applicable, transfers of personal information to a third country or an international organization, including the identification of that third country or international organization;
- where possible, the envisaged time limits for erasure of the different categories of personal information;
- where possible, a general description of the technical and organizational security measures used to protect the personal information.

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

The privacy team is responsible for ensuring that such records are maintained across all Group Members who process personal information protected by the General Data Protection Regulation, and will liaise as necessary with appropriate managers within each group member to create and maintain such records.

21. 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**").

22. Internal Complaint Mechanisms

Any individual whose personal information is subject to these Rules may raise any privacy-related compliance questions, issues or concern that a Group Member 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 Group Members in connection with the Rules on request to the privacy team at privacy1@motorolasolutions.com.

23. Responsibility for breaches by non-EEA group members

Dansk Beredskabskommunikation AS will be responsible for ensuring that any action necessary is taken to remedy any breach of these Rules by a non-EEA Group Members.

In particular:

- In the event of a claim being made in which the relevant individual has suffered any material or non-material damage because of a breach of these Rules by a non-EEA Group Member, Dansk Beredskabskommunikation AS will have the burden of proof to show that the non-EEA Group Member is not responsible for the breach, or that no such breach took place.
- where a non-EEA Group Member fails to comply with these Rules, individuals may exercise their rights and remedies above and bring any claim they may have in relation to a breach of these Rules by a non-EEA Group Member against Dansk Beredskabskommunikation AS and, where appropriate, receive compensation from Dansk Beredskabskommunikation AS for such breach.

24. 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, Group Members accept that both Dansk Beredskabskommunikation AS and the

processor may be held liable for the entire damage in order to ensure effective compensation of the individual.

25. Mutual assistance and cooperation with Supervisory Authorities

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 a Supervisory Authority with competent jurisdiction in accordance with the Cooperation Procedure (see Appendix 5).

Each Group Member shall cooperate with a competent Supervisory Authority in accordance with the Cooperation Procedure (see Appendix 5).

26. Relationship between national laws and the Rules

Where a Group Member has reason to believe that the legislation applicable to the Group Member is likely to prevent the Group Member from fulfilling its obligations under the Rules or has a substantial effect on the guarantees provided by the Rules, the Group Member should promptly inform Dansk Beredskabskommunikation AS 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). Dansk Beredskabskommunikation AS and the Privacy & Data Security Compliance Committee will determine a suitable course of action aimed at ensuring compliance with the BCR and if a legal requirement a Group Member is subject to is likely to have a substantial adverse effect on the guarantees provided under the Rules, report the issue to the relevant Supervisory Authority (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.

27. Third party beneficiary rights for Data Subjects and Liability

This section "Third party beneficiary rights for Data Subjects and Liability" applies where individuals' personal information are protected under EEA data protection laws (including the 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 EEA;
- a non-EEA Group Member (or its third-party processor) offers goods and services (including free goods and services) to those individuals in the EEA; or
- a non-EEA Group Member (or its third-party processor) monitors the behavior of those individuals, as far as their behavior takes place in the EEA; and
- that Group Member then transfers those individuals' personal information to a non-EEA 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:

- 5 Transparency and Fairness
- 7 Special Category Personal Data
- 8 Data Transfers outside EEA
- 9 Purpose Limitation
- 10 Data quality, proportionality and storage limitation
- 11 Transfers to third parties
- 12 Publication of the Rules
- 13 Individual's data protection rights
- 15 The right to object to receiving marketing information
- 16 Automated individual decisions
- 17 Security and confidentiality of data
- 21 Records of data processing
- 22 Data Protection by Design and Default
- 23 Internal Complaint Mechanisms
- 24 Responsibility for breaches by non-EEA Group Members
- 25 Shared liability for breaches with processors
- 25 Mutual assistance and cooperation with Supervisory Authorities

- 26 Relationship between national laws and the Rules
- 27 Third party beneficiary rights for EEA Data Subjects and Liability
- 30 Government Requests for Disclosure of Personal Information

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

- *Complaints:* Individuals may make a complaint to the Privacy Team and/or to the competent Supervisory Authority in accordance with the Complaints Handling Procedure at Appendix 4;
- *Proceedings:* Individuals, in accordance with their rights to an effective judicial remedy, may bring proceedings against a Group Member in accordance with the Complaints Handling Procedure at Appendix 4; and/or
- *Liability:* Individuals may seek appropriate redress from Dansk Beredskabskommunikation AS including the remedy of any breach of the Rules by any Group Member outside the EEA and, where appropriate receive compensation from Dansk Beredskabskommunikation AS for any material or non-material 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.

28. Compliance and supervision of compliance

As part of its commitment to ensuring compliance with the Rules and to respecting individuals' rights to privacy, Group Members have 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. The functional representatives 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, Group Members have trained and designated data privacy champions and EU privacy points of contact, who are responsible for tracking compliance with country privacy laws, with support from regional legal representatives and/or the privacy team including the Group Members' Data Protection Officer.

Group Members' Privacy and Data Security Compliance Committee, Data Protection Officer and extended regional privacy team must ensure that Group Members are 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, informing and advising Group Members and their staff on their obligations under applicable data protection laws;
- monitoring compliance by Group Members with applicable data protection laws and data protection policies of the Group Member;
- awareness raising and training of staff involved in processing;
- providing data protection advice to the business units on a day-to-day basis and project basis, including advising on data protection impact assessments;
- acting as contact point for Supervisory Authorities, consulting with Supervisory Authorities where required by applicable data protection laws and
- assisting with Supervisory Authorities' requests for information or cooperation and managing local requests for information held about them by individuals and complaints.

The Data Protection Officer exercises their tasks independently and reports directly to the highest levels of management. In carrying out their tasks as Data Protection Officer they have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purpose of processing. Individuals may contact the Data Protection Officer with regard to all issues relating to processing of their Personal Information, including exercising any of their data protection rights. The Data Protection Officer can be contacted by email at: privacy1@motorolasolutions.com.

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

Group Members 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 Danish Data Protection Authority and any other relevant Supervisory Authorities and non-material changes will be communicated to the Danish

Data Protection Authority and any other relevant Supervisory Authorities at least once a year. Group Members will also provide a brief explanation of the reasons for any notified changes to the Rules.

Group Members 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 Dansk Beredskabskommunikation AS 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 Supervisory Authorities on request. Dansk Beredskabskommunikation AS 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. Group Members 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 Danish Data Protection Authority and any other relevant Supervisory Authorities where required.

The Rules became effective on May 2, 2013 and were transferred from the UK Supervisory Authority to the Danish Supervisory Authority on [DATE] 2021. The Rules apply to all personal information processed by Group Members or its service providers on or after that date and the Rules will take precedence over any other policies or procedures within Group Members relating to the collection and use of personal information.

30. 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.