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.

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 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 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

Binding Corporate Rules:

Appendix 2 - Fair Information Disclosures

1. Background

1.1 These Controller Binding Privacy Rules (“Rules") provides a framework for the transfer of personal information between Group Members.

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

2. Information to be provided where Group Members collect personal information directly from individuals

2.1 When Group Members collect personal information directly from individuals, they must provide the following transparency information in a privacy notice:

(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 Group Members' or a third party's legitimate interests, the **legitimate interests** pursued by Group Members 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 EEA intends to **transfer** personal information to a third country or international organization outside of the EEA, 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, Group Members 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 competent Supervisory Authority;

(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 the Group Members obtain the personal information from the individual. If the Group Member intends to further process personal information for a purpose other than that for which it was originally collected, before starting the new processing, the Group Member will provide a privacy notice to the individual to notify them of the new purpose and to provide the information described above at paragraph 2.2.

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

3.1 When Group Members 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 **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 Group Members' or a third party's legitimate interests, the **legitimate interests** pursued by Group Members or by the third party;

(e) the categories of **personal information** that are being processed;

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

(g) where applicable, the fact that a Group Member in the EEA intends to **transfer** personal information to a third country or international organization outside of the EEA, 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.

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

(i) 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;

(j) 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;

(k) the right to **lodge a complaint** with the competent Supervisory Authority;

(l) 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; and

(m) **details of the source** from which Group Members 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 Group Members 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.

3.3 If the Group Member intends to further process personal information for a purpose other than that for which it was originally collected, before starting the new processing the Group Member will provide a privacy notice to the individual to notify them of the new purpose and to provide the information described above at paragraph 3.2.

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 Group Members 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 Group Members 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 Group Members is subject, including a statutory obligation of secrecy.

Motorola Solutions

Binding Corporate Rules:

Appendix 3 -

Data Subject Rights Procedure

1. Background

1.1 Motorola Solutions' 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 Group Members under the Rules have certain data protection rights, which they may exercise by making a request to the controller of their information (where the controller is a Group Member) (a "**Data Protection Rights Request**").

1.3 This Binding Corporate Rules: Data Protection Rights Procedure ("**Procedure**") describes how Group Members will respond to any Data Protection Rights Requests they receive from individuals whose personal information are processed and transferred under the Rules.

2. Individual's data protection rights

2.1 Group Members 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 a Group Member to make any Data Protection Rights Request then where the Group Member 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 the Group Member is a controller or processor of the personal information that is the subject of the request;

(b) where the Privacy team determines that the Group Member 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 the Privacy team determines that the Group Member 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 the Privacy team determines that a Group Member 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 may be made in writing, which can include email, or 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 the Group Member 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. The Group Member 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 The Group Member 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 The Group Member 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). In the

case of manifestly unfounded or excessive requests, the Group Member may alternatively charge a reasonable fee.

3.4.3 A Group Member will not be required to comply with a Data Protection Rights Request if it can demonstrate it is not in a position to identify the individual making the request.

3.5 *Responding to a Data Protection Rights Request*

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

3.5.2 The Group Member 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.

3.5.3 If the Group Member decides not to take action on the Data Protection Rights Request, the Group Member 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 competent Supervisory Authority and seeking a judicial remedy.

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 a competent Supervisory Authority;

(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 EEA, the appropriate safeguards that the Group Member has put in place relating to such transfers in accordance with applicable data protection laws.

4.1.2 An individual is also entitled to 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 Group Member 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 the Group Member 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 an EEA Group Member transfers personal information under the Controller Policy, if the refusal to provide the information is consistent with the applicable data protection law in the EEA Member State where the Group Member is located). For example, where a request is manifestly unfounded or excessive the request may be refused or alternatively a reasonable fee charged;

(b) where the personal information is not subject to applicable data protection law. For example, personal information held by a Group Member in non-automated form that is not or will not become part of a filing system will not be subject to the General Data Protection Regulation;

(c) the personal information does not originate from the EEA, has not been processed by any EEA Group Member, and the provision of the personal information requires a Group Member 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 a Group Member 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 a Group Member 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 a Group Member must rectify or erase personal information in its capacity as controller, the Group Member 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.

The right to rectification and correction of personal information

5.4 Requests from individuals to rectify inaccurate personal information must be complied with by Group Members without undue delay. Taking into account the purposes of the processing, Group Members must also comply with requests from individuals to complete incomplete personal information, which may be by including a supplementary statement.

The right to restriction of personal information

5.5 Requests from individuals to restrict their personal information must be complied with by Group Members without undue delay if:

(a) The accuracy of personal information is contested;

(b) The processing of their personal information is unlawful but the individual does not want their personal information deleted;

(c) The personal information is no longer needed by the Group Member but the individual requires the personal information to establish, exercise or defend legal claims; or

(d) Pending verification of whether the legitimate interests of the Group Member override those of the individual, if the individual has objected to processing of their personal information.

5.6 If personal information has been restricted, other than to store the personal information, the Group Member must not process the personal information unless it is with the individual's consent, to establish, exercise or defend legal claims, protect the rights of other individuals or legal persons or for reasons of important public interest.

5.7 Group Members will inform the relevant individual before lifting the processing restriction.

The right to erasure of personal information

5.8 Unless an exemption applies (these are listed below), if a request to erase information is received from an individual, the Group Member must comply with the request without undue delay if any of the following grounds apply:

5.8.1 The information is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

5.8.2 The individual withdraws the consent on which the processing is based and the Group Member has no other legal ground for the processing;

5.8.3 The processing is on the basis of performance of a task in the public interest or in the exercise of official authority vested in the Group Member or is on the basis of legitimate interests pursued by the Group Member or a third party and the individual objects to the processing and there are no overriding legitimate grounds for the processing;

5.8.4 The personal information has been unlawfully processed;

5.8.5 The personal information must be erased to comply with a legal obligation under European Union or Member State law which the Group Member is subject to;

5.8.6 The personal information was collected in relation to the offer of information society services to children; or

5.8.7 The processing is for direct marketing purposes and the individual objects to receiving direct marketing.

5.9 If a Group Member 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.

Exemptions from the right to erasure

5.10 Group Members will not be required to comply with an erasure request if the processing is necessary:

5.10.1 To exercise the right of freedom of expression of information;

5.10.2 To comply with a legal obligation under European Union or Member State law which a Group Member is subject to:

5.10.3 In the public interest relating to public health;

5.10.4 For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or

5.10.5 To establish exercise or defend legal claims.

6. Requests for data portability

6.1 If an individual makes a Data Protection Rights Request to a Group Member acting as controller to receive the personal information that he or she has provided to a Group Member in a structured, commonly used and machine-readable format and/or to transmit directly such information to another controller (where technically feasible), the Group Member's 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 or is carried out by automated means.

6.2 This right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

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 a Group Member acting as controller not to be subject to automated decision making (including profiling), the 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 Group Member Data Protection Office or at privacy1@motorolasolutions.com.

Motorola Solutions

Binding Corporate Rules:

Appendix 4 - Complaint Handling Procedure

February 14, 2022

1. Background

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

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

1.3 This procedure will be made available to individuals whose personal information is processed by Group Members 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 the Group Member's Privacy Team at privacy1@motorolasolutions.com.

3. Complaints where Group Member 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 a Group Member 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.

3.2.3 If the Group Member does not take action on the individual's request, the Privacy Team will inform the individual of the reasons for not taking action without delay and at the latest within one (1) month. In which case, the individual has the right to lodge a complaint with the competent Supervisory Authority and to bring a claim before the courts.

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 competent Supervisory Authority and to commence proceedings

4.1 *Overview*

4.1.1 Where individuals' personal information:

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

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

then those individuals (whether they are in or outside of the EEA) 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 a competent Supervisory Authority (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 a Group Member under this Complaints Handling Procedure.

4.1.3 Group Members accept that complaints and claims made pursuant to paragraphs 5.2 and 5.3 may be lodged by a non-for-profit body, organization or association acting on behalf of the individuals concerned.

4.2 *Complaint to a Supervisory Authority*

4.2.1 If an individual wishes to complain about a Group Member's processing of his or her personal information to a Supervisory Authority, on the basis that an EEA 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 EEA Group Member to the Supervisory Authority in the EEA territory:

(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 a Group Member's processing of his or her personal information to a Supervisory Authority, on the basis that a non-EEA Group Member has processed personal information in breach of the Rules or in breach of applicable data protection laws, then Dansk Beredskabskommunikation AS will be subject to the jurisdiction of the competent Supervisory Authority in place of that non-EEA Group Member, as if the alleged breach had been caused by Dansk Beredskabskommunikation AS.

4.3 *Proceedings before a national court*

4.3.1 If an individual wishes to commence court proceedings against a Group Member, on the basis that an EEA 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 EEA Group Member in the EEA territory:

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

(b) of his or her habitual residence.

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

Motorola Solutions

Binding Corporate Rules:

Appendix 5 - Cooperation Procedure

February 14, 2022

1. Background

1.1 Motorola Solutions' Binding Corporate Rules: Cooperation Procedure sets out the way in which Group Members will cooperate with competent Supervisory Authorities in the European Economic Area in relation to the Group Member Binding Corporate Rules (Controller Policy) ("**the Rules**").

2. Cooperation Procedure

2.1 Where required, Group Members will make the necessary personnel available for dialogue with a competent Supervisory Authority in relation to the Rules.

2.2 Group Members will provide upon request copies of the results of any audit it conducts of the Rules to a competent Supervisory Authority, who will treat the audit results in accordance with any confidentiality obligations applicable to the Supervisory Authority under applicable data protection law.

2.3 Group Members agree that a competent Supervisory Authority may audit any Group Member who processes personal information as a controller for compliance with the Rules.

2.4 Group Members agree to take into account the advice of and abide by a formal decision of any competent Supervisory Authority 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 a Group Member chooses to exercise including any right of appeal.

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

Motorola Solutions

Binding Corporate Rules:

Appendix 6 - Privacy Training Requirements

February 14, 2022

1. Background

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

1.2 The document sets out the requirements for Group Members to train their staff members on the requirements of the Rules.

1.3 Group Members 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 applicable data protection laws, including EEA 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 Group Members' Privacy team has overall responsibility for privacy training at Group Members, 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 The senior management of Group Members 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 Group Members' 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 the Group Member 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 Group Members 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 Group Member 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 Group Members' 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 Group Members internationally?

(e) What are Group Members' 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

Binding Corporate Rules:

Appendix 7 - Government Data Request Procedure

1. Background

1.1 Motorola Solutions' Binding Corporate Rules: Government Data Request Procedure sets out Group Members' 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 Group Members (hereafter "**Data Disclosure Request**").

1.2 Where a Group Member 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, Group Members 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, Group Members do 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, Group Members will notify and cooperate with the competent Supervisory Authorities (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 Group Member receives a Data Disclosure Request, the recipient of the request must pass it to the Group Members' Data Protection Officer, immediately upon receipt, indicating the date on which it was received together with any other information which may assist the Group Members' 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 The Group Members' Data Protection Office will carefully review each and every Data Disclosure Request on a case-by-case basis. The Group Members' 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 competent Supervisory Authorities*

4.1.1 The Group Member will put the request on hold in order to notify and consult with the competent Supervisory Authorities, 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 competent Supervisory Authorities will include information about the data requested, the requesting body, and the legal basis for the disclosure. Where the Group Member is not reasonably able to notify the relevant Supervisory Authorities of a Data Disclosure Request due to imminent risk of serious

harm, provided the Group Member is not legally prohibited from doing so, the Group Member will notify the competent Supervisory Authorities when it is reasonably able to do so.

4.1.2 Where a Group Member is prohibited from notifying the competent Supervisory Authorities and suspending the request, the Group Member 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 the Group Member can consult with the competent Supervisory Authorities, which may also, in appropriate circumstances, include seeking a court order to this effect. The Group Member will maintain a written record of the efforts it takes.

5. Transparency reports

5.1 If, despite having used its best efforts, the Group Member is not in a position to notify the competent Supervisory Authorities, the Group Member 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. The Group Member shall provide this report to the lead Supervisory Authority which authorized its BCR (and any other Supervisory Authorities that the lead Supervisory Authority may direct) 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

Binding Corporate Rules:

Appendix 8 –

Material Scope of the Controller Policy

1. Background

1.1 The “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 European Economic Area (“EEA”) may transfer the personal information that they control described in this section to every other Group Member inside and outside of the EEA.** **Every Group Member outside of the EEA may also transfer the personal information that they control described in this section to every Group Member inside and outside of the EEA.**
Who receives this personal information?	**Every Group Member outside of the EEA may receive the personal information described in this section which is sent to them by other Group Members inside and outside of the EEA.** **Every Group Member inside of the EEA may also receive the personal information described in this section which is sent to them by other Group Members inside and outside of the EEA.**

What categories of personal information are transferred?	**Group Members collect and transfer the following categories of personal information:** **· Name and contact details including email, address (home and work) and phone number** **· National identifiers such as national I.D., tax ID and passport number** **· Emergency contact** **· Bank account details** **· Compensation information (including pay, bonus and benefits)** **· Pension entitlement and payments** **· Performance reviews and disciplinary information** **· CV or resume, qualifications, date of birth, references** **· Driving licence records, security clearance status, visa or immigration status** **· IT data (device ID, IP address, password, logs, software use tracking information (i.e., cookies and information recorded for security, operation and training purposes).** **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?	**1. Past and current staff** **2. Individual consultants** **3. Independent contractors** **4. Temporary staff** **5. 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. For further detail in relation to key data servers, centers and applications see the addendum to this Appendix 8.

3. Customer relationship management data

Who transfers the personal information described in this section?	Every Group Member inside of the European Economic Area ("EEA") may transfer the personal information that they control described in this section to every other Group Member inside and outside of the EEA. Every Group Member outside of the EEA may also transfer the personal information that they control

	described in this section to every Group Member inside and outside of the EEA.
Who receives this personal information?	**Every Group Member outside of the EEA may receive the personal information described in this section which is sent to them by other Group Members inside and outside of the EEA.** **Every Group Member inside of the EEA may also receive the personal information described in this section which is sent to them by other Group Members inside and outside of the EEA.**

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.** **For further detail in relation to key data servers, centers and applications see the addendum to this Appendix 8.**

4. Supply chain management data

Who transfers the personal information described in this section?	**Every Group Member inside of the European Economic Area ("EEA") may transfer the personal information that they control described in this section to every other Group Member inside and outside of the EEA.** **Every Group Member outside of the EEA may also transfer the personal information that they control described in this section to every Group Member inside and outside of the EEA.**
Who receives this personal information?	**Every Group Member outside of the EEA may receive the personal information described in this section which is sent to them by other Group Members inside and outside of the EEA.** **Every Group Member inside of the EEA may also receive the personal information described in this section which is sent to them by other Group Members inside and outside of the EEA.**

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.** **For further detail in relation to key data servers, centers and applications see the addendum to this Appendix 8.**

Addendum to Appendix 8 – Material Scope of the BCR

Key Data Servers / Centers / Applications	System App Location	MSI Location Where Data Can Be Accessed Internally	Type of Data (HR, Supply Chain Management Data, Customer Relationship Support Data)
Active_Directory	US	Global - permissions based	HR
ACCESSDATA_FTK	US	Global - permissions based	IT
AIRES_MOBILITY	US	Global - permissions based	HR
AKAMAI	US	Global - permissions based	IT
AMDOCS_SMART CLIENT	US	Global - permissions based	IT
AON-HEWITT	US	Global - permissions based	HR
APPLICATION_SECURITY_TRAINING	US	Global - permissions based	HR
APPTIO_IT COST TRANSPARENCY APPLICATION SUITE	US	Global - permissions based	IT
APTTUS	US	Global - permissions based	Customer Relationship Support Data & Suppy Chain Management Data
ATG_KNOWLEDGE	US	Global - permissions based	HR
ATLASSIAN_JIRA	US	Global - permissions based	IT
AUDITTOOL_EMS_QUALITY	US	Global - permissions based	HR
AXIELL_MIMSY XG	US	Global - permissions based	Marketing
AXIS	US	Global - permissions based	IT
AZURE_ACTIVE_DIRECTORY	US	Global - permissions based	HR
BATCHAT	US	Global - permissions based	HR
BIT9 PARITY SUITE	US	Global - permissions based	IT
BRIO_MANAGEMENT SUMMARY	US	Global - permissions based	Customer Relationship Support Data
CDM_CLOUD	US	Global - permissions based	Customer Relationship Support Data
CYBERGRANTS	US	Global - permissions based	HR
CYBERSOURCE_ECOMMERCE PAYMENT SERVICES	US	Global - permissions based	Customer Relationship Support Data
DAMGAARD_CONCORDE EUROPE	US	Global - permissions based	Customer Relationship Support Data
DELOITTE_PAYROLL_	Romania	Global - permissions based	HR
E_BOKS	Denmark	Global - permissions based	HR
ENDPOINT_PROTECTOR_DLP	US	Global - permissions based	IT

ENDPOINT_SECURITY_SCORECARD	US	Global - permissions based	IT
ENTRUST_IDENTITYGUARD	US	Global - permissions based	IT
ETRADE	US	Global - permissions based	HR
GESBANHA	Portugal	Global - permissions based	HR
GETTHERE_MOT GETTHERE SSO CORP	US	Global - permissions based	HR
GOOGLE_WORKSPACE	US	Global - permissions based	HR
GUIDANCE SOFTWARE_ENCASE	US	Global - permissions based	IT
IBM_BIGFIX_PATCH_MANAGEMENT	US	Global - permissions based	IT
IEXPENSE	US	Global - permissions based	HR
INS ZOOM_INS ZOOM	US	Global - permissions based	HR
INTERSET	US	Global - permissions based	IT
MOON SOFTWARE_PASSWORD AGENT	US	Global - permissions based	IT
MOT_ACCOUNTING OPERATIONS REVIEW	US	Global - permissions based	HR
MOT_BOARD MEMBERSHIP TRACKING	US	Global - permissions based	HR
MOT_CORE DIRECTORY	US	Global - permissions based	HR
MOT_DYNALIST	US	Global - permissions based	HR
MOT_ETHICS TRACKER	US	Global - permissions based	HR
MOT_MY VACATION	US	Global - permissions based	HR
MOT_PERSONNEL DATABASE	US	Global - permissions based	HR
MOT_S3D TIMESHEET SYSTEM	US	Global - permissions based	HR
OKTA SINGLE SIGN-ON	US	Global - permissions based	HR
ORACLE_ELOQUA_MARKETING AUTOMATION PLATFORM	US	Global - permissions based	Customer Relationship Support Data
ORACLE_MOTOROLA_APPLICATION_DIRECTORY_LDAP	US	Global - permissions based	HR
PBS_PAYROLL	Spain	Global - permissions based	HR
PROOFPOINT_EMAIL_BACKBONE	US	Global - permissions based	HR
SALESFORCE.COM_CHANNEL_SALES	US	Global - permissions based	Customer Relationship Support Data
SALESFORCE.COM_DIRECT_SALES	US	Global - permissions based	Customer Relationship Support Data

SALESFORCE.COM_SALES_LEAD MANAGEMENT	US	Global - permissions based	Customer Relationship Support Data
SALESFORCE.COM_SALES_MARKE T PLACE	US	Global - permissions based	Customer Relationship Support Data
SALESFORCE.COM_SALES_PRESAL ES_RESOURCE_REQUEST	US	Global - permissions based	Customer Relationship Support Data
SD WORX_PAYROLL	Austria, Belgium, Denmark, France, Germany, Greece, Hungary, Ireland, Italy, Netherlands, Poland, Portugal, Sweden	Global - permissions based	HR
SYMANTEC_ENDPOINT PROTECTION	US	Global - permissions based	HR
WEB MONEY	US	Global - permissions based	HR
WIRELESS MGMT ETOOL	US	Global - permissions based	HR
WORKDAY	US	Global - permissions based	HR
ZALARIS_TIME TRACKING	Sweden	Global - permissions based	HR
ZPL13_HR_TOOLS_PLATNIK	Poland	Global - permissions based	HR