



Intel Binding Corporate Rules:

EEA Controller BCR

Last Updated: June 2026

Contents

Part I: Introduction.....	2
Part II: Our obligations	8
Part III: Delivering compliance in practice	34
Part IV: Third-Party Beneficiary Rights.....	40
Part V: Appendices.....	44

Part I: Introduction

This Intel Binding Corporate Rules EEA: Controller BCR ("**Controller BCR**") establishes Intel's approach to compliance with European data protection laws when processing personal data for its own purposes as a controller.

Scope of this Controller BCR

Article 44 of the European Union ("**EU**") General Data Protection Regulation ("**GDPR**") prohibits transfers of personal data to a country or international organization outside the European Economic Area unless a European Commission adequacy determination applies (pursuant to Article 45 of the GDPR), the data exporter and data importer have implemented appropriate safeguards (pursuant to Article 46 of the GDPR), or a derogation applies (pursuant to Article 49 of the GDPR).

This Controller BCR therefore applies only to transfers of personal data in the circumstances above, i.e., transfers of personal data between Intel group companies as controllers (or where a group member acts as processor on behalf of another group member) that are restricted pursuant to Article 44 of the GDPR. It provides appropriate safeguards for the personal data that are transferred between those group members pursuant to Articles 46(1) and 46(2)(b) of the GDPR. This Controller BCR applies regardless of whether our group members process personal data by manual (when it forms part of a filing system or is intended to form part of a filing system) or by automated means.

For an explanation of some of the terms used in this Controller BCR, like "controller", "process", "processor", and "personal data", please see the section headed "Important terms used in this Controller BCR" below.

Types of personal data within the scope of this Controller BCR

This Controller BCR applies to all personal data that we process as a controller, including personal data processed in the course of our business activities, employment administration, and vendor management:

- **Human resources data:** including personal data of past and current employees, individual consultants, independent contractors, temporary workers, and job applicants;
- **Customer relationship management data:** including personal data relating to representatives of i) business customers who use our business services and products and ii) potential customers; and
- **Supply chain management data:** including personal data of individual contractors and of account managers and workers of third-party suppliers who provide products and services to us.

Appendix 11 (Material Scope of the Controller BCR) sets out a more detailed description of the personal data and the intra-group transfers that are covered by this Controller BCR.

Our collective responsibility to comply with this Controller BCR

All group members and their workers must comply with and respect this Controller BCR when processing personal data as a controller, irrespective of the country in which they are located. All group members (listed in Appendix 1) have agreed to be bound by and fully comply with this Controller BCR by executing the Intel Intra-Group Agreement (dated 19 September 2021) or by acceding to the Intel Intra-Group Agreement through the execution of a Statement of Adherence. No transfer of personal data shall be made to an Intel company under this Controller BCR until the company is effectively bound by and can comply with this Controller BCR.

In particular, all group members who process personal data as a controller must comply with:

- the rules set out in **Part II** of this Controller BCR;
- the practical commitments set out in **Part III** of this Controller BCR;
- the third-party beneficiary rights set out in **Part IV**; and
- the policies and procedures appended in **Part V** of this Controller BCR.

Workers are made aware of such requirements and the sanctions in case of non-compliance in various ways, including, where applicable, via internal policies, which workers are required to observe. Workers also complete annual training on the Controller BCR, and, following this training, the workers commit to complying with the Controller BCR.

Management commitment and consequences of non-compliance

Intel's management is fully committed to ensuring that all group members and their workers comply with this Controller BCR at all times.

Non-compliance may cause Intel to be subject to sanctions imposed by competent supervisory authorities and courts and may cause harm or distress to individuals whose personal data have not been protected in accordance with the practices described in this Controller BCR.

In recognition of the gravity of these risks, workers who do not comply with this Controller BCR may be subject to disciplinary action, up to and including dismissal. Workers are made aware that anybody who violates the law may also be subject to civil and criminal penalties.

Upon withdrawal of a group member from this Controller BCR, the group member and any internal or external processor shall delete or return all the personal data processed pursuant to this Controller BCR and delete the copies thereof according to Intel's then-applicable data retention and disposal policies. If the applicable law in the third country in which the group member is located requires the group member or any internal or external processor to continually store the personal data, then the group member and any internal or external processors shall agree with the group member exporting the personal data that the personal data may be retained by the group member. The group member shall warrant that: (i) the personal data will be retained in accordance with the provisions of Rule 13; and (ii) it will, and will ensure any internal or external processors will, guarantee the confidentiality of the personal data and will not further process the personal data other than as required by the relevant law.

Where will this Controller BCR be made available?

This Controller BCR is accessible on Intel's corporate website at: <https://www.intel.com/content/www/us/en/privacy/eea-binding-corporate-rules.html>.

Important terms used in this Controller BCR

For the purposes of this Controller BCR:

- the term **applicable data protection laws** means the EU General Data Protection Regulation 2016/679 ("GDPR") and any other European data protection laws that apply to transfers of personal data under this Controller BCR;

- the term **applicable EU laws** means the laws made by the EU and the laws of any European country (as European is defined below);
- the term **competent supervisory authority** means the supervisory authority competent for the group member exporting personal data from Europe and “competent supervisory authorities” shall be construed accordingly;
- 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 data. For example, Intel is a controller of its Human Resources records and Customer Relationship Management records;
- the term **criminal personal data** means information about an individual's criminal offenses or convictions;
- the term **data exporter** means the Intel group member exporting personal data or otherwise making personal data available to the data importer;
- the term **data importer** means the Intel group member outside Europe that receives or otherwise has access to personal data from the data exporter;
- the term **Europe** (and **European**) as used in this Controller BCR refers to the Member States of the European Economic Area – that is, the Member States of the European Union plus Norway, Liechtenstein, and Iceland;
- the term **group member** means the members of Intel's group of companies listed in Appendix 1;
- the term **personal data** means any information relating to an identified or identifiable natural person. An identifiable natural person 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 natural person;

- the term **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, 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 data on behalf of a controller (for example, a third-party service provider that is processing personal data in order to provide Intel a service or an Intel company that is providing services to another Intel company that is a controller);
- the term **sensitive 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 **supervisory authority** means an independent public authority that is established by a European country pursuant to the GDPR to be responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within Europe;
- the term **workers** refers to all employees, new hires, individual contractors, and consultants and temporary workers engaged by any Intel group member. All workers must comply with this Controller BCR.

How to raise questions or concerns

If you have any questions regarding this Controller BCR, your rights under this Controller BCR or applicable data protection laws or any other data protection issues, you can contact Intel's Privacy Office using the details below. Intel's Privacy Office will either address the matter directly or forward it to the appropriate person or department within Intel to respond.

Contact: Intel Privacy Office

Webform: <https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html>

Address: Intel Corporation

Attention: Intel Privacy Office

2200 Mission College Boulevard

Santa Clara, CA 95054

USA

OR

Intel Ireland Limited

Attention: Intel Privacy Office

Collinstown Industrial Park

Leixlip

Co.Kildare

Ireland

W23 CX68

Intel's Privacy Office is responsible for ensuring that changes to this BCR are notified to the group members and to individuals whose personal data are processed by Intel in accordance with Appendix 9 (Updating Procedure).

If you want to exercise any of your data protection rights, please see the data protection rights procedure set out in Appendix 3 (Data Protection Rights Procedure). Alternatively, if you are unhappy about the way in which Intel has used your personal data, you can raise a complaint in accordance with our complaint handling procedure set out in Appendix 7 (Complaint Handling Procedure).

Part II: Our obligations

This Controller BCR applies in all situations where a group member processes personal data anywhere in the world. All workers and group members must comply with the following obligations:

Rule 1 – Lawfulness:	We will at all times comply with any applicable data protection laws, as well as the practices set out in this
<i>We will ensure that processing is at all times compliant with applicable law and this Controller BCR.</i>	Controller BCR, when processing personal data. As such, where applicable data protection laws exceed the standards set out in this Controller BCR, we will comply with those laws.

Rule 2 – Fairness and transparency:	We will provide individuals the Fair Information Disclosures (see Appendix 2) when we process their personal data. We will publish this Controller BCR in full
<i>We will inform individuals how and why their personal data will be processed.</i>	on our website. We will take appropriate measures to communicate the Fair Information Disclosures to individuals in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. 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. If we have not obtained personal data directly from the individual themselves then, in certain limited cases, we might not need to provide the Fair Information Disclosures, as explained in Appendix 2 . Where this is the case, the Intel Privacy Office must be informed and will decide what course of action is appropriate to

protect the individual's rights, freedoms, and legitimate interests.

Rule 3 – Lawful basis for processing

We will only process personal data if at least one of the following grounds is fulfilled:

- (a) the data subject has given consent to the processing of personal data for one or more specific purposes after receiving, in clear and plain language, all necessary information;
- (b) processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary to protect the vital interests of the data subjects or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- (f) processing is necessary to pursue the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

which require protection of personal data, in particular where the data subject is a child.

Rule 4 – Purpose limitation:

We will process personal data only for specified, explicit, and legitimate purposes and not further process that information in a manner that is incompatible with those purposes.

We will only process personal data for specified, explicit, and legitimate purposes that have been communicated to the individuals concerned in accordance with Rule 2. We will not process personal data in a way that is incompatible with those purposes, except in accordance with applicable data protection laws or with the individual's consent.

If we intend to process personal data for a purpose incompatible with the purpose for which the personal data were originally collected, we may only do so if such further processing is permitted by applicable data protection laws or we have the individual's consent. We will also provide the individual Fair Information Disclosures about the further processing in accordance with Rule 2.

In assessing whether any processing is compatible with the purpose for which the personal data were originally collected, we will take into account:

- any **link** between the purposes for which the personal data were originally collected and the purposes of the intended further processing;
- the **context** in which the personal data were collected and, in particular, the reasonable

expectations of the individuals whose personal data will be processed;

- the **nature** of the personal data, in particular whether such information constitutes sensitive personal data and/or criminal personal data;
- the **possible consequences** of the intended further processing for the individuals concerned;
- the existence of any **appropriate safeguards** that we have implemented in both the original and intended further processing operations; and
- whether further processing is for **archiving purposes** in the public interest, scientific, or historical research purposes or statistical purposes, which shall not be considered to be incompatible with the initial purposes.

Rule 5 – Data minimization:

We will only process personal data that are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

We will only process personal data that are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. We will not process personal data that are unnecessary to achieve those purposes.

Rule 6 – Accuracy: <i>We will keep personal data accurate and, where necessary, up to date.</i>	We will take appropriate measures to ensure that the information we process is accurate and, where necessary, kept up to date – for example, by giving individuals the ability to inform us when their personal data have changed or become inaccurate. We will take reasonable steps to ensure inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without undue delay.
Rule 7 – Storage limitation: <i>We will only keep personal data for as long as is necessary for the purposes for which they are collected and further processed.</i>	We will not keep personal data in a form which permits identification of individuals for longer than is necessary for the purposes for which that information is processed. In particular, we will comply with Intel's record retention policies and guidelines as revised and updated from time to time.
Rule 8 – Security, integrity, and confidentiality: <i>We will implement appropriate technical and organizational measures to apply a level of security to personal data that is appropriate to the risk for the rights and freedoms of the individuals.</i>	We will implement appropriate technical and organizational measures designed to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and all other unlawful forms of processing. In particular, we will comply with the requirements in the security policies in place within Intel, as revised and updated from time to time, together with any other

security procedures relevant to a business area or function.

These security policies and procedures are designed to take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymization and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and
-

organizational measures for ensuring the security of the processing.

Any worker who has access to or is involved in the processing of personal data will do so only on instructions from the Intel company on whose behalf the processing is being carried out and under a duty of confidence.

Rule 9 – Data protection by design and by default

We will apply data protection by-design and by-default principles when we design and implement new products and systems that process personal data.

We adopt internal policies and implement appropriate measures, which meet the principles of data protection by-design and data protection by-default. This means that:

(a) both at the time of the determination of the means for processing and at the time of the processing itself, we will implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Controller BCR and ensure the protection of the rights of the data subjects; and

(b) we will implement appropriate technical and organizational measures for ensuring that, by default, only those personal data are processed that are necessary for each specific purpose of the processing and are not collected or retained beyond the minimum necessary for those purposes, both in terms of the

amount of the personal data and the time of their storage. We will ensure that, by default, personal data are not made accessible to an indefinite number of individuals.

Rule 10 – Service provider management:

We will ensure that our service providers also adopt appropriate security measures when processing personal data.

Where we appoint a service provider to process personal data on our behalf (i.e., an internal or external processor), we will impose strict contractual terms on the service provider that require it to:

- act only on our documented instructions when processing that information, including with regard to international transfers of personal data;
- maintain policies so that any individuals who have access to the data are subject to a duty of confidence;
- have in place appropriate technical and organizational security measures to safeguard the personal data;
- only engage a sub-processor if we have given our prior specific or general written authorization and on the condition that: (i) the sub-processor agreement protects the personal data to the same standard required of the service provider; and (ii) the service provider

	remains fully liable to us for the performance of the sub-processor’s data protection obligations; • assist us in complying with our obligations as a controller under applicable data protection laws, in particular with respect to i) reporting data security incidents under Rule 11, ii) responding to requests from individuals to exercise their data protection rights under Rule 12, and iii) conducting Data Protection Impact Assessments (and, where required, to consult with supervisory authorities) under Section 5 of Part III of this Controller BCR; • return or permanently destroy the personal data once it has completed its services and delete existing copies unless applicable law requires storage of the data; and • make available to us all information we might need in order to ensure its compliance with these obligations and allow for and contribute to audits, including inspections, conducted by us or another auditor we mandate.
--	--

Rule 11 – Data Incident Reporting: <i>We will comply with any data incident reporting requirements that exist under applicable law.</i>	When we become aware of an incident that might present a risk to the personal data in our custody or control, we will promptly and without undue delay inform Intel’s Privacy Office, which will initiate Intel’s Privacy Incident Response procedures and inform the
---	--

Intel controller. (Any notifications to the Intel Privacy Office are deemed to be a notification to Intel Ireland Limited.)

The Intel Privacy Office will review the nature and seriousness of the data incident, commence an appropriate investigation aligned with the circumstances, and determine whether it is necessary under applicable data protection laws to notify competent supervisory authorities.

In particular:

- If the incident is likely to result in a risk to the rights and freedoms to individuals whose personal data were affected by the incident, the Intel Privacy Office shall notify competent supervisory authorities without undue delay and, where feasible, within 72 hours, in accordance with applicable data protection laws.
- If the incident is likely to result in a high risk to individuals whose personal data were affected by the incident, the Intel Privacy Office shall notify those individuals without undue delay in accordance with applicable data protection laws.

The Intel Privacy Office shall be responsible for confirming that any such notifications, where necessary, are made in accordance with applicable data protection law and shall make any documentation relating to a breach available to the competent supervisory authority on request. All data incidents should be documented (comprising the facts relating to the breach, its effects, and the remedial action taken) in a data-breach register.

Rule 12 – Honoring individuals' data protection rights:

We will enable individuals to exercise their data protection rights in accordance with applicable law.

European laws provide individuals certain data protection rights. These include:

- *The right of information:* This is a right for an individual to have certain information provided or made available by the controller, including the identity and contact details of the controller or its representatives, the purposes of processing data and/or any transfers outside Europe, the lawful basis and legitimate basis for processing personal data, the intended recipients for such personal data, and the period of time for which the personal data will be stored.
 - *The right of access:* This is a right for an individual to obtain confirmation whether we process personal data about them and, if so, to
-

be provided details of that personal data and access to the personal data.

- *The right to rectification:* This is a right for an individual to obtain rectification without undue delay of inaccurate personal data we might process about them.
 - *The right to erasure:* This is a right for an individual to request that we erase personal data about them on certain grounds (set out in [Appendix 3](#)) – for example, where the personal data are no longer necessary to fulfill the purposes for which they were collected. If we have made the personal data public, then (taking account of available technology and the cost of implementation) we will also take reasonable steps, including technical measures, to inform controllers processing the personal data that the individual has requested the erasure by such controllers of any links to, or copy or replication of, that personal data.
 - *The right to restriction:* This is a right for an individual to require us to restrict processing of personal data about them on certain grounds (set out in [Appendix 3](#)).
 - *The right to data portability:* This is a right for an individual to receive personal data concerning
-

them from us in a structured, commonly used and machine-readable format and to transmit that information to another controller, if certain grounds apply (set out in [Appendix 3](#)). Where technically feasible, this may include direct transmission from Intel to another controller.

- *The right to object:* This is a right for an individual to object, on grounds relating to their particular situation, to processing of personal data about them, if certain grounds apply (set out in [Appendix 3](#)).
 - *The right not to be subject to decision based solely on automated processing, including profiling:* see Rule 16.
 - *The right to withdraw consent:* This is a right for an individual to withdraw their consent at any time where the processing of their personal data is based on consent.
 - *The right to lodge a complaint through Intel's internal complaint process:* This is a right to lodge a complaint through Intel's internal complaint process ([Appendix 7](#))
 - *The right to lodge a complaint with a supervisory authority:* This is a right to lodge a complaint with a supervisory authority if the individual
-

considers that the processing of personal data relating to them infringes this Controller BCR.

- *The right to effective judicial remedy:* This is a right of an individual to an effective judicial remedy where they consider that their rights under the GDPR have been infringed as a result of the processing of their data in non-compliance with this Controller BCR.
- *The right to seek redress and compensation:* The right to seek redress and compensation, where appropriate, for a breach of this Controller BCR.

Where an individual wishes to exercise any of their data protection rights, we will respect those rights in accordance with applicable data protection laws by following the Data Protection Rights Procedure (see [Appendix 3](#)). Further detail on the right to lodge a complaint or issue legal proceedings are set out in ([Appendix 7](#)).

In addition, the relevant Intel group member shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with this rule to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. We will inform the individual about those recipients if the individual requests it.

Rule 13 – Ensuring adequate protection for international transfers:

We will not transfer personal data internationally without ensuring adequate protection for the information in accordance with applicable law.

Data transfer compliance

No group member may transfer or onward transfer personal data internationally unless and until it complies with this Rule 13 by ensuring that i) there are enforceable data subject rights and effective legal remedies for individuals (unless a data transfer derogation applies) and ii) a Transfer Impact Assessment has been conducted where necessary.

European laws prohibit international transfers of personal data to third countries unless i) the country has been deemed to provide an adequate level of protection, ii) appropriate safeguards are in place so that the transferred data remain protected to the standard required in the country or region from which they originally transferred, and enforceable data subject rights and effective legal remedies for individuals are available, iii) a data transfer derogation applies under applicable data protection laws, or iv) the individual has explicitly consented to the transfer. This includes transfers of personal data to group members who are subject to this Controller BCR and transfers (and onward transfers) from group members to third parties who are not subject to this Controller BCR.

Appropriate safeguards may include: i) standard data protection clauses (i.e., the Standard Contractual Clauses) adopted by the European Commission, ii)

standard data protection clauses adopted by a supervisory authority and approved by the European Commission, iii) an approved code of conduct together with binding and enforceable commitments of the recipient to apply the appropriate safeguards, including as regards data subjects' rights, or iv) an approved certification mechanism together with binding and enforceable commitments of the recipient to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of an adequacy decision or appropriate safeguards, the transfer may take place only if one of the following conditions applies: i) the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the individual due to the absence of an adequacy decision and appropriate safeguards, ii) the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the individual's request, iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the controller and another natural or legal person, iv) the transfer is necessary for important reasons of public interest, v) the transfer is necessary for the establishment, exercise, or defense of legal claims, vi) the transfer is necessary in order to protect the vital interests of the

individual or of other persons, where the individual is physically or legally incapable of giving consent, or vii) the transfer is made from a register that, according to EU or Member State law, is intended to provide information to the public and is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

Transfer Impact Assessments

Where the GDPR applies to the personal data that will be transferred (or onward transferred), then before a data exporter makes an international transfer (or onward transfer) of personal data to a data importer (which is either a group member or, for the purposes of this rule, any third-party recipients), the Intel Privacy Office must coordinate with the data importer to undertake a risk assessment to ensure there is no reason to believe that the laws and practices in the country where the data importer will process the personal data, including any requirements to disclose personal data or measures authorizing access by public authorities, will conflict with Intel's obligations under this Controller BCR (a "**Transfer Impact Assessment**"). These assessments will be based on the understanding that laws and practices that respect the essence of the

fundamental rights and freedoms of individuals, and do not exceed what is necessary and proportionate in a democratic society to safeguard national security, defense, or public security, are not in contradiction with this Controller BCR. Before a data exporter may rely on this Controller BCR for a transfer of personal data outside Europe, the data exporter will commit that they have no reason to believe that the laws and practices in the non-European country of destination applicable to the data importer (including any requirements to disclose personal data or measures authorizing access by public authorities) prevent the data importer from fulfilling its obligations under this Controller BCR. The Intel Privacy Office shall liaise with the data exporter, as necessary, to conduct the Transfer Impact Assessment, and address its findings. A Transfer Impact Assessment does not need to be undertaken for each transfer, and one assessment may apply to the same transfer of a specific type of data to the same country.

No international transfer (or onward transfer) of personal data may take place unless and until: i) a Transfer Impact Assessment has been conducted and ii) any additional safeguards that are identified as necessary pursuant to the Transfer Impact Assessment to protect the transfer of personal data to the data importer have been implemented by the data exporter and data importer.

The Transfer Impact Assessment must take due account in particular of the following elements:

- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer or set of transfers occurs; the location of the processing and storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorizing access by such authorities, including those providing for access to these data during the transit between the country of the data exporter and the country of the data importer – relevant in light of the specific circumstances of the transfer and the applicable limitations and safeguards; and
 - (iii) any relevant contractual, technical, or organizational safeguards put in place to supplement the safeguards under this Controller BCR, including measures applied during transmission and to the processing of the personal data in the country of destination.
-

The Intel Privacy Office shall inform other relevant group members about the findings of the Transfer Impact Assessment, so that they can apply any identified additional safeguards determined to be necessary in respect of any identical or similar transfers they make.

The data exporter, along with Intel Ireland Limited and the Intel Privacy Office, commits to promptly identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or the data importer in order to enable them to fulfill their obligations under this Controller BCR. The same applies if a data exporter has reason to believe that a data importer can no longer fulfill its obligations under this Controller BCR. Where the Transfer Impact Assessment concludes that it is not possible to implement additional safeguards to ensure the data importer's processing in the third country will be compatible with the requirements of this Controller BCR, then the Intel Privacy Office shall inform the data exporter (and other relevant group members) and shall prohibit any such transfer by the group member(s).

The data importer must use its best efforts to provide the Intel Privacy Office relevant information and continue to cooperate with the Intel Privacy Office to ensure compliance with the requirements of this

Controller BCR throughout the duration of the transfer and subsequent processing. In the case of a third-party data importer, the Intel Privacy Office must exercise appropriate diligence to ensure that the third-party data importer has used such best efforts and will continue to provide such cooperation, including, where appropriate, by seeking contractual assurances from the third-party data importer.

The Intel Privacy Office will coordinate with the third-party data importer to i) document the Transfer Impact Assessment and the supplementary measures selected and implemented and ii) make the documentation available to the competent supervisory authority on request, as well as to select and implement the appropriate supplementary measures.

The Intel Privacy Office will inform relevant group members of the assessment carried out and the results of that assessment for the purposes of identifying supplementary measures that might need to be put in place (in case the same type of transfer is carried out by any other group member) or when relevant transfers or categories of transfers may be suspended or ended.

For the third countries to which the data exporters have transferred personal data, the data exporters must monitor on an ongoing basis, and where appropriate in collaboration with data importers, developments that could affect the initial assessment of the level of

protection and the actions accordingly taken on such transfers.

Transfer Risk Notifications

The data importer must promptly notify the Intel Privacy Office and the data exporter if, at any time during which it receives or processes personal data from the data exporter, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of this Controller BCR, including following a change in the laws of the third country where it receives or processes personal data or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements of this Controller BCR (a “**Transfer Risk Notification**”). In the case of a third-party data importer, the Intel Privacy Office must exercise appropriate diligence to ensure that the third-party data recipient will provide any such Transfer Risk Notification, including where appropriate by seeking contractual assurances from third-party data importer. The Intel Privacy Office shall further assess the laws and practices of any third country to which it transfers personal data on a regular basis to ensure that any such transfers do not become incompatible with the obligations under this Controller BCR. For the third countries to which the data exporter has transferred personal data, this will include, in collaboration with

data importers where appropriate, assessing developments that could affect the initial assessment of the level of protection and the actions accordingly taken on such transfers.

Following receipt of a Transfer Risk Notification from the data importer, or if the Intel Privacy Office or the data exporter otherwise has reason to believe that the data importer's processing is (or is at risk of becoming) incompatible with the obligations under this Controller BCR, the Intel Privacy Office shall promptly identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The Intel Privacy Office shall instruct the data exporter to suspend the data transfer if i) it considers that no appropriate safeguards for such transfer can be ensured or ii) the data exporter is instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate its transfers of personal data to the data importer, insofar as it concerns the processing of personal data under this Controller BCR (in which event, the data importer must be required to return or destroy the personal data it received, as instructed by the data exporter, and should certify the deletion of the data to the data exporter). Until the data are deleted or returned, the data importer should continue to ensure compliance with this Controller BCR or its contractual

commitments. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with this Controller BCR and will only process the data to the extent and for as long as required under that local law. If the data exporter transfers personal data to two or more data importers, the data exporter may exercise this right to terminate only with respect to the relevant data importer.

Rule 14 – Sensitive Personal Data and/or Criminal Personal Data:

Intel will assess whether sensitive personal data are required for the intended purpose of processing before collecting them.

We will only process sensitive personal data and/or criminal personal data collected where we have obtained the individual's explicit consent, unless there is an alternative legitimate basis for processing consistent with applicable law.

In principle, we will obtain the individual's explicit consent to collect and process their sensitive personal data, unless we have another legitimate basis for doing so consistent with the applicable data protection laws of the country in which the personal data were collected. Examples of such legitimate bases are where:

- processing is necessary in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the individual where the data

-
-
- subject is physically or legally incapable of giving consent;
 - processing relates to personal data which are manifestly made public by the individual;
 - processing is necessary for the establishment, exercise or defense of legal claims;
 - processing is necessary for reasons of substantial public interest on the basis of applicable, EU law;
 - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or European country law or pursuant to contract with a health professional;
 - processing is necessary for reasons of public interest in the area of public health; or
 - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR based on applicable, EU laws.

Processing of criminal personal data shall only be carried out under the control of official authority or where authorized by applicable data protection laws

	providing for appropriate safeguards for the rights and freedoms of individuals. When obtaining an individual's explicit consent, that consent will be given freely, and will be specific, informed, and unambiguous.
Rule 15 – Direct marketing: <i>We will allow customers to opt out of receiving marketing information.</i>	All individuals have the right to object, in an easy-to-exercise manner and free of charge, to the use of their personal data for direct-marketing purposes, and we will honor all such opt-out requests.
Rule 16 – Automated individual decision-making, including profiling: <i>We will respect individuals' rights not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them.</i>	We will not make any decision, which produces legal effects concerning an individual or that similarly significantly affects them, based solely on the automated processing of that individual's personal data, including profiling, unless such decision is: • necessary for entering into or performing a contract between a group member and that individual; • authorized by applicable laws; or • based on the individual's explicit consent. In the first and third cases above, we will implement suitable measures to protect the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention, to express their view, and to contest the decision.

	We will never make automated individual decisions about individuals using their sensitive personal data, unless they have given explicit consent under Rule 14 or another lawful basis applies.
--	---

Part III: Delivering compliance in practice

So that we follow the rules set out in this Controller BCR, in particular the obligations set out in Part II, Intel and all of its group members will also comply with the following practical commitments:

1. Resourcing and compliance:

We will have appropriate resourcing and support to ensure and oversee privacy compliance throughout the business.

The Intel Privacy Office is responsible for overseeing and enabling compliance with this Controller BCR on a day-to-day basis.

A summary of the roles and responsibilities of Intel's privacy team is set out in [Appendix 4](#) (Privacy Compliance Structure).

2. Privacy training:

We will ensure workers are educated about the need to protect personal data in

Group members will provide appropriate and up-to-date privacy training to workers who:

- have regular access to personal data; or
 - are involved in the processing of personal data or in the development of products, services, and/or tools that process personal data.
-

<i>accordance with this Controller BCR</i>	We will provide such training in accordance with the Privacy Training Program (see Appendix 5).
3. Records of Data Processing: <i>We will maintain records of the data processing activities under our responsibility.</i>	We will maintain a record of the processing activities that we conduct in accordance with applicable data protection laws. These records should be kept in writing (which might be in electronic form), and we will make these records available to competent supervisory authorities upon request. The Intel Privacy Office is responsible for ensuring that such records are maintained.
4. Audit: <i>We will conduct data protection audits on regular basis.</i>	We will conduct data protection audits on a regular basis, which may be conducted by either internal or external accredited auditors. In addition, we will conduct data protection audits on specific request from the Ethics and Compliance Oversight Committee, Internal Audit, the Data Protection Officer, the Intel Privacy Office, or any internal legal advisors. We will conduct any such audits in accordance with the Audit Protocol (see Appendix 6).
5. Data Protection Impact Assessments: <i>We will conduct data protection impact assessments where processing is likely to result in a high risk to rights and freedoms of individuals and consult with competent supervisory</i>	Where required by applicable data protection laws, we will conduct data protection impact assessments (“DPIA”) whenever the processing of personal data, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. Prior to processing, Intel will conduct a DPIA, which will contain at least the following: • A systematic description of the envisaged processing operations and the purposes of the processing;

<i>authorities where required by applicable law.</i>	• An assessment of the necessity and proportionality of the processing operations in relation to the purposes; • An assessment of the risks to the privacy rights of individuals; • The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and demonstrate compliance with applicable data protection laws.
	Where the DPIA indicates that the processing would still result in a high risk to individuals, Intel will consult with local supervisory authorities where required by applicable data protection laws.
6. Privacy by design and by default:	When designing and implementing new products and systems that process personal data, we will apply data protection by-design and by-default principles. This means we will implement appropriate technical and organizational measures that:
<i>We will apply data protection by-design and by-default principles when we design and implement new products and systems that process personal data.</i>	• 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 data necessary for each specific processing purpose are

	collected, stored, processed, and accessible; in particular, that, by default, an individual's personal data are not made accessible to an indefinite number of people without the individual's intervention (" privacy by default ").
7. Complaint handling: <i>We will enable individuals to raise data protection complaints and concerns.</i>	Group members will enable individuals to raise data protection complaints and concerns (including complaints about processing under this Controller BCR) by complying with the Complaint Handling Procedure (see Appendix 7).
8. Cooperation with competent supervisory authorities: <i>We will always cooperate with competent supervisory authorities.</i>	Group members will cooperate with competent supervisory authorities by complying with the Cooperation Procedure (see Appendix 8).
9. Updates to this Controller BCR: <i>We will update this Controller BCR in accordance with our Updating Procedure</i>	Whenever updating our Controller BCR, we will comply with the Updating Procedure (see Appendix 9).
10. Non-compliance with this Controller BCR and conflicts	If a group member acting as data importer breaches or is unable to comply with this Controller BCR for any reason, the group member should promptly inform the Intel Privacy Office and suspend the relevant transfer where

between this Controller BCR and national legislation:

We will assess non-compliance with this Controller BCR, take care where local laws conflict with this Controller BCR, and act responsibly to ensure a high standard of protection for the personal data in such circumstances.

possible. If the data importer cannot ensure compliance with this Controller BCR within one month of the suspension of the data transfer, the data importer should, at the election of the data exporter, immediately return or delete the relevant personal data in their entirety and otherwise follow the procedure in Rule 13 of Part II of this Controller BCR.

If local laws applicable to any group member prevent it from fulfilling its obligations under the Controller BCR or otherwise have a substantial effect on its ability to comply with the Controller BCR, the group member will promptly notify the Intel Privacy Office (which notice will be considered a notification to Intel Ireland Limited) unless prohibited by a law enforcement authority.

The Intel Privacy Office, in consultation with Intel Ireland Limited, will make a responsible decision on the action to take and will, where appropriate, consult with the competent supervisory authority.

In addition, where a group member is subject to national legislation of a non-European territory that conflicts with this Controller BCR in the manner described above, the Intel Privacy Office will also inform Intel Ireland Limited.

When undertaking an international transfer of personal data, group members must comply with the requirements of Rule 13 of Part II of this Controller BCR to minimize the likelihood and risk of any such conflict arising in the first place.

Where the data importer is in persistent breach of the BCR or fails to comply with a binding decision of a competent court or supervisory authority, the data exporter may request the immediate return or deletion of the personal data that have been transferred under this Controller BCR in their entirety. The same commitments should apply to any copies of the personal data. The data importer should certify the deletion of the personal data to the data exporter. Until the data are deleted or returned, the data importer should continue to ensure compliance with this Controller BCR. In the case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with this Controller BCR and will only process the data to the extent and for as long as required under that local law.

11. Government requests for disclosure of personal data:

We will notify the competent supervisory authorities in case of a legally binding request for disclosure of personal data.

If a group member receives a legally binding request for disclosure of personal data subject to this Controller BCR or otherwise becomes aware of direct access to personal data by a law enforcement authority or state security body, it will comply with the Government Data Request Response Procedure set out in [Appendix 10](#).

Part IV: Third-Party Beneficiary Rights

Application of this Part IV

This Part IV applies where individuals' personal data are protected under European data protection laws (including the GDPR). This occurs when:

- those individuals' personal data are processed in the context of the activities of a group member (or its third-party processor) established in Europe;
- a non-European group member (or its third-party processor) offers goods and services (including free goods and services) to those individuals in Europe; or
- a non-European group member (or its third-party processor) monitors the behavior of those individuals, as far as their behavior takes place in Europe;

and that group member then transfers those individuals' personal data to a non-European group member for processing under the Controller BCR.

All individuals shall be provided information on their third-party beneficiary rights regarding the processing of their personal data and the means to exercise those rights.

Third-party beneficiary rights

Every individual whose personal data are protected under European data protection laws shall have a right to enforce, as a third-party beneficiary, the following provisions of this Controller BCR:

- (a) duty to respect the general data protection principles relating to transparency, fairness, and lawfulness; purpose limitation; legal basis for processing; processing of special categories of data; data minimization and limited storage periods; data protection by design and by default; data accuracy; security and data breach notification; and onward transfers of data (Rules 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 13, and 14 of Part II);

- (b) duty to ensure transparency and easy access to this Controller BCR by ensuring all data subjects are provided information on i) how their data are processed, ii) their third-party beneficiary rights and the means to exercise those rights, iii) how they can hold an Intel company liable, and iv) the data protection principles described in (a) of this section of Part IV (Rule 2 of Part II);
- (c) duty to respect rights of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right to withdraw consent, and right not to be subject to decisions based solely on automated processing (including profiling) (Rules 12, 15 and 16 of Part II);
- (d) duty to assess whether national legislation prevents fulfilment of the obligations under this Controller BCR before data transfers take place and on an ongoing basis (Rule 13 of Part II, section 10 of Part III);
- (e) duty to be transparent if national legislation prevents an Intel company from fulfilling its obligations under this Controller BCR, including any legally binding request for disclosure of personal data by a law enforcement authority or state security body (section 11 of Part III);
- (f) duty to respect the right to complain through the internal complaint mechanism (section 7 of Part III and Appendix 7);
- (g) duty to cooperate with concerned supervisory authorities to ensure compliance by group members with this Controller BCR (section 8 of Part III and Appendix 8);
- (h) duty to inform individuals of any update to this Controller BCR (section 9 of Part III and Appendix 9);
- (i) with respect to the liability provisions under which individuals may enforce this Controller BCR against an Intel company, Intel Ireland Limited accepts responsibility for actions of a group member outside Europe and agrees to pay compensation for damages resulting from the violation of this Controller BCR by such group member (Part IV);
- (j) this third-party beneficiary rights provision (Part IV); and
- (k) the remedies set out in Appendix 7 and in this Part IV (i.e., to lodge a complaint or seek redress and compensation).

These rights do not extend to those elements of this Controller BCR pertaining to internal mechanisms, such as details of training, audit program, compliance network, and mechanism for updating this Controller BCR.

Entitlement to effective remedies

When this Part IV applies, individuals have the right to pursue effective, judicial remedies in the event their personal data are processed by Intel in breach of the following provisions of this Controller BCR:

- Part II (Our Obligations) of this Controller BCR;
- Sections 7 (Complaints Handling), 8 (Cooperation with Competent Supervisory authorities), 10 (Non-compliance with this Controller BCR and Conflicts between this Controller BCR and national legislation), and 11 (Government requests for disclosure of personal data) under Part III of this Controller BCR; and
- Part IV (Third-Party Beneficiary Rights) of this Controller BCR.

Right to judicial remedies, redress, and compensation

When this Part IV applies, individuals may exercise the following rights:

- *Complaints*: Individuals may complain to a group member and/or to a European supervisory authority, in accordance with the Complaints Handling Procedure at Appendix 7;
- *Proceedings*: Individuals may commence proceedings against a group member for violations of this Controller BCR, in accordance the Complaints Handling Procedure at Appendix 7;
- *Compensation*: Individuals who have suffered material or non-material damage as a result of an infringement of this Controller BCR have the right to receive compensation from Intel for the damage suffered.
- *Transparency*: Individuals also have the right to obtain a copy of the Controller BCR via: <https://www.intel.com/content/www/us/en/privacy/eea-binding-corporate-rules.html>.

Data subjects shall have the right to mandate a not-for-profit body, organization, or association that has been properly constituted in accordance with the law of a European Member State, has statutory objectives in the public interest, and is active in the field of the protection of data

subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on their behalf and to exercise the rights referenced in this Part IV of this Controller BCR on their behalf where provided by applicable, European law.

Responsibility and liability for breaches by non-European group members

When this Part IV applies, Intel Ireland Limited will be responsible for ensuring that any action necessary is taken to remedy any breach of this Controller BCR by a non-European group member.

In particular:

- If an individual can demonstrate damage it has suffered likely occurred because of a breach of this Controller BCR by a non-European group member, Intel Ireland Limited will have the burden of proof to show that the non-European group member is not responsible for the breach or that no such breach took place.
- Where a non-European group member fails to comply with this Controller BCR, individuals may exercise their rights and remedies against Intel Ireland Limited and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Intel Ireland Limited for any material or non-material damage suffered as a result of a breach of this Controller BCR. Intel Ireland Limited accepts responsibility for actions of all group members outside Europe and agrees to pay compensation for damages resulting from the violation of this Controller BCR by such group member outside Europe.

Shared liability for breaches with processors

When this Part IV applies, where Intel 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 this Controller BCR, Intel accepts that both Intel and the processor may be held liable for the entire damage in order to ensure effective compensation of the individual.

Part V: Appendices

APPENDIX 1

INTEL GROUP MEMBERS

EEA Entities

Name of entity	Registered address	Registration Number
Austria		
Intel Austria GmbH (LE:543)	Europastraße 8, Building T02, 9524 Villach, Austria	FN 351052 d
Belgium		
Intel Corporation NV/SA (LE:300)	Kings Square, Veldkant 31, 2550 Kontich, Belgium	0415.497.718
Czech Republic		
Intel Czech Tradings Inc (Czech Branch) (LE:470)	I.Pavlova 1789/5, 120 00 Prague 2 Czech Republic	60165898
Denmark		
Intel Mobile Communications Denmark ApS (LE:306)	Hørkær 12A, 2730 Herlev, Denmark	CVR No. 33163150
Finland		
Intel Finland OY (LE:350)	Westendinkatu 7, Espoo, 02160, Finland	0357606-4
France		
Intel Corporation SAS (LE:330)	Les Montalets, 2, rue de Paris, 92196, Meudon Cedex, France	302 456 199

Silicon Mobility (LE: 334)	535 Route des Lucioles, Les Aqueduc's, Batiment 2, 06560, Sophia Antipolis, Valbonne, France	815 085 659
-------------------------------	--	-------------

Germany		
Intel Deutschland GmbH (LE:356)	Am Campeon 10-12, 85579, Neubiberg, Germany	HRB 186928
Intel Germany Services GmbH (LE:346)	Am Campeon 10, 85579, Neubiberg, Germany.	HRB 262579
Intel Germany GmbH & Co. KG (LE:342)	Lilienthalstrabe 15, D-85579, Neubiberg, Germany	HRA 94167
Intel Magdeburg GmbH (LE:365)	Am Campeon 10, 85579, Neubiberg, Germany	HRB 31356

Ireland		
Intel Research and Development Ireland Limited (LE:508)	Collinstown Industrial Park, Leixlip, Co.Kildare, Ireland	308263
Intel Ireland Limited (external company) (LE:500)	Collinstown Industrial Park, Leixlip, Co.Kildare, Ireland	E902934
Codeplay Europe Limited (LE:413B)	Collinstown Industrial Park, Leixlip, Kildare, Ireland	689761
Grange Newco LLC (Irish Branch Office) (LE:377)	Collinstown Industrial Park, Collinstown, Kildare, W23 CX68, Ireland	910178
Italy		
Intel Corporation Italia S.p.A. (LE:360)	Milanofiori, Palazzo, E/4, 20057, Assago (Milano), Italy)	04236760155
Lithuania		
Intel Vilnius UAB (LE:366)	J.Jasinskio 16B, LT-03163 Vilnius, Lithuania	UI 2000-105. Co. ID No. 11169
Netherlands		
Intel Benelux B.V. (LE:390)	High Tech Campus 83, 5656AG, Eindhoven, Netherlands	24134020
Intel International B.V. (LE:540)	Capronilaan 37, 1119 NG, Schiphol-Rijk, Netherlands	34098535
Intel Finance BV (LE:398)	Capronilaan 37, 1119 NG, Schiphol-Rijk, Netherlands	57978972
Intel International Finance BV (LE:976)	Capronilaan 37, 1119 NG, Schiphol-Rijk, Netherlands	18037530

Poland		
Intel Technology Poland Sp. Z o.o. (LE:466)	ul. Slowackiego 173, 80-298, Gdansk, Poland	KRS 101882
Intel Wroclaw sp. z o.o. (LE: 467)	ul. Słowsackiego 173, 80-298, Gdańsk, Poland	KRS 0001004817
Portugal		
Turbe – Distribucão e Marketing de Produtos Electronicos, Sociedade Unipessoal, Lda. (LE:370)	Rua Castilho, 44, 8 th floor, 1250-071 Lisbon, Portugal	505 456 036
Romania		
Intel Software Development S.R.L. (LE:474)	2A Piața Consiliul Europei, United Business Center 1, 7 th floor unit U1E7 and 8 th floor, Timișoara, Timiș county, Romania	J35/340/2017 27555127
Spain		
Intel Corporation Iberia S.A. (LE:320)	Martinez Villergas, 49, Bloque V, Planta 1, Oficina 134, Martinez Villergas Business Park, 28027, Madrid, Spain	CIF A-28819381
Sweden		
Intel Sweden A.B. (LE:400)	Isafjordsgatan 30B, 16440 Kista, Sweden	556189-6027

Non-EEA Entities

Name of entity	Registered address	Registration number
Argentina		

Intel Software de Argentina S.A. (LE:221)	Juan Díaz de Solís 1330, 5 th floor, Vicente López, Province of Buenos Aires, Buenos Aires, Argentina	30-70944960-1
Australia		
Intel Australia Pty. Ltd. (LE:932)	Level 61, Governor Phillip Tower, 1 Farrer Place, Sydney NSW 2000, Australia	001 798 214
Brazil		
Intel Semicondutores do Brasil Ltda. (LE:220)	Av. Dr. Chucri Zaidan, 940, 9o, 10o, e 11o andares, Vila Cordeiro, Sao Paulo, 04583904, Brazil	142882
Canada		
Intel Technology of Canada, ULC (LE:200)	Suite 1700, Park Place, 666 Burrard Street, Vancouver BC V6C 2X8, Canada	C1312651
Cayman Islands		
Intel Ireland Limited (LE: 505)	190 Elgin Avenue, George Town, Grand Cayman, KY1-9008, Cayman Islands	32967
Grange Newco LLC (LE: 327)	c/o Walkers Corporate Limited, 190 Elgin Ave, George Town, Grand Cayman, KY1-9008 Cayman Islands	6795
Chile		
Intel Tecnologia El Chile S.A. (LE:229)	211 El Bosque Norte Ave, 1 st Floor, Las Condes, Santiago, Chile	Fojas 20763 16606 Year 2000
China		
Intel Asia-Pacific Research & Development Ltd. (LE:764)	No. 880 Zi Xing Road, Zizhu Science Park, Shanghai, 201109, China	913100007659516415

Intel China Ltd. (LE:776)	2/F, No. 751 Zi Ri Road, Zizhu Science Park, Shanghai, 200241, China	310000400073046
Intel China Ltd, Beijing Branch (LE:776A)	20/F, Tower D, Beijing Global Trade Center, No. 36, North Third Ring Road East, Beijing, Dong Cheng District, 100013, China	91110101X000399926
Intel China Ltd, Chengdu Branch (LE:776U)	Room 1701-1709, F17, Building 3, No. 1199, North part of Tianfu Avenue, High-tech Zone, Chengdu, Sichuan, China	91510100MA61W9LB13
Intel China Ltd. Shanghai Branch (LE:776H)	23rd Floor, ShanghaiMart Tower, No. 2299 Yan'an Road (West), Shanghai, 200336, China	913100007818987806
Intel China Ltd. Shenzhen Branch (LE: 776C)	3-5 Floor, Block 3, Viseen Business Park, No.43 Gaoxin South Loop Road, High-tech Zone Community, Yuehai Subdistrict, Nanshan District, Shenzhen, China	91440300738839558W
Intel China Ltd. Xi'an Hi-tech Zone Branch (LE: 776V)	ET603-101, 6F, East Tower, Ascendas Innovation Towers, No.88 West of 6th Keji Road, Hi-tech Zone, Xi'an, Shaanxi Province, China	91610131MAB0X733XA
Intel China Research Center Ltd. (LE:725)	8F, Raycom Infotech Park A, No.2, Kexueyuan South Road, Beijing, Haidian District, 100190, China	91110108761401095K
Intel Integrated Circuit (Hainan) Ltd. (LE: 702)	Room 910/901, Sunshine Financial Plaza, No. 360-1, Yingbin Road, Jiyang District, Sanya, Hainan Province, China	91460000MAC5RX1M7M

Intel Products (Chengdu) Ltd. (LE:778)	No. 8-1, Kexin Road, Chengdu High-Tech Zone, Chengdu, Sichuan, 611731, China	91510100752809830T
Intel Semiconductor (Dalian) Ltd. (LE:724)	No. 109 Huaihe Road East, Dalian Economic and Technology Development Area, Dalian, Liao Ning Province, 116600, China	91210200787321704D
Intel Trading (Shanghai) Co., Ltd. (LE:888)	Room 317, 3th Floor, No. 2 Middle Tainan Road, Waigaoqiao Free Trade Zone, Pudong, Shanghai, 200131, China	913100006073880990
Intel Mobile Communications Technology (Shanghai) Ltd. Beijing Branch (LE: 891A)	Room A329, 3rd Floor, Building 1, No. 36 North Third Ring East Road, Dongcheng District, Beijing China	91110101MAD5GL3RXX
Intel Mobile Communications Technology (Shanghai) Ltd. Chengdu Branch (LE:891C)	Unit 1402, Building 3, No. 1199 North Section of Tianfu Ave, Chengdu Hi-Tech Zone, Chengdu, China	91510100MAD18K4EXT
Intel Mobile Communications Technology (Shanghai) Ltd. Shenzhen Branch (LE: 891D)	15H, A8 Music Building, No. 99, Gaoxin South 9th Road, Binhai Community, Yuehai Subdistrict, Nanshan District, Shenzhen, China	91440300MAD0K13R2D
Intel Mobile Communications Technology (Shanghai) Ltd. Xi'an Branch (LE:891E)	Room 622, 6/F, Block A, Ascendas Innovation Hub, No.38, Gaoxing No. 6 Road, Xi'an Hi-Tech Zone, Xi'an, Shannxi Province, China	9161131MAD18EL238
Colombia		

Intel Tecnologia de Colombia S.A. (LE:224)	Cra. 7 No. 71-21 Torre B Of. 603, Bogota, Cundinamarca, Colombia	830034293
Costa Rica		
Componentes Intel de Costa Rica, S.A. (LE:230)	S.A. Avenida Escazú, Torre Lexus, 4to piso. Escazú, San Jose, Costa Rica, Costa Rica	3-102-186874
Intel Free Trade Zone Park, S.A. (LE:233)	Bufete Facio & Canas, Forum 2 Business Center, Pacheco Coto Building 4 th Floor, Costa Rica	3-101-385965
Manufactura Ensamble & Pruebas EMP Intel de Costa Rica Sociedad de Responsabilidad Limitada (LE:247)	Calle 129, Province Heredia, Belen, San Antonio, Zona Franca Belen, Costa Rica	4062001213633
Egypt		
Intel Corporation Egypt LLC (LE:665)	Office No 444, Administrative Building No 47, Fourth Floor, Al Tassein North Street, Fifth Settlement, New Cairo, Egypt	20390
Hong Kong		
Intel Asia Holding Limited (LE:761)	69/F, Central Plaza, 18 Harbour Road, Wanchai, Hong Kong	856307
Intel Semiconductor Limited (LE:765)	Suite 6803, 68/F, Central Plaza, 18 Harbour Road, Wanchai, Hong Kong	06463822

Intel Semiconductor (US) LLC (Hong Kong branch) (LE:760A)	69/F, Central Plaza, 18 Harbour Road, Wanchai, Hong Kong	F8920
Intel China Finance Holding (HK) Ltd (LE:904)	Suite 6803, 68/F, Central Plaza, 18 Harbour Road, Wanchai, Hong Kong	61775834
India		
Intel Technology India Private Limited (LE:831)	23-56P, Deverabeesanahalli, Varthur Hobli, Outer Ring Road, Bangalore, Karnataka, 560 103, India	U85110KA1997PTC021606
Intel Solutions & Services India Private Limited (LE:834)	23-56P, Deverabeesanahalli, Varthur Hobli, Outer Ring Road, Bangalore, Karnataka, 560 103, India	U32105KA2002PTC030832
Indonesia		
Intel Indonesia Corporation – Jakarta Representative Office (LE:850)	Regus Menara BCA, Grand Indonesia, Menara BCA 45 th & 50 th Floor, Jl. MH Thamrin No 1 Kel. Menteng, Kecamatan Menteng, Jakarta Pusat, 10310, Indonesia	SIT.2396/A/P3A/DJPDN/VI/98
Israel		
Intel Electronics Ltd. (LE:600)	Shderot Hahavatz st #11, Industrial Area, Kiryat-Gat, Israel	PC-51-085443-3
Intel Israel Limited (LE:620)	Andrei Saharov 9 Street Haifa, 3508409, Israel	PC 51-068286-7

Intel Mobile Communications Israel Ltd. (LE:625)	94 Em Hamoshavot Rd, Petach-Tikva, Israel	P.C. 51-291090-2
Intel Semi Conductors Ltd. (LE:640)	P.O. Box 498, Haifa, 31000, Israel	PC-51-078931-6
Granulate Cloud Solutions Ltd. (LE: 604)	4 Yigal Alon St., Tel Aviv, 6789139, Israel	515898982
Habana Labs Ltd (LE:615)	9 Granit Street, Caesarea, Israel	51-5361327
Japan		
Intel Kabushiki Kaisha (LE:650)	Kokusai Bldg. 5F, 1-1, Marunouchi 3chome, Chiyoda-ku, Tokyo, 100-0005, Japan	0100-01-122400
Kenya		
Intel Corporation (UK) Ltd. (Kenya Branch) (LE:462)	Office no. 2, 4 th Floor, Cavendish Block Riverside Drive (off Chiromo Road) Nairobi City Kenya	88/2008
Malaysia		
Intel Microelectronics (M) Sdn. Bhd. (LE:755)	1 st Floor, 2 Lebuh Pantai, 10300 George Town, Penang, Malaysia	199401016571 (302251-K)
Intel Products (M) Sdn. Bhd. (LE:745)	1 st Floor, 2 Lebuh Pantai, 10300 George Town, Penang, Malaysia	199501036533 (365735-X)

Intel Technology Sdn. Berhad (LE:750)	1st Floor, 2 Lebuah Pantai, 10300 George Town, Penang, Malaysia	197701005406 (36420-H)
Intel Electronics Malaysia Sdn Bhd (LE:870)	1st Floor, 2 Lebuah Pantai, 10300 George Town Penang, Malaysia	199601005832 (378178-K)
Intel MSC Sdn. Bhd (LE: 735)	1st Floor, 2 Lebuah Pantai, 10300 George Town, Penang, Malaysia	199601010958 (383307-P)
Mexico		
Intel Tecnologia de Mexico S. de R.L de C.V. (LE:154)	Blvd. Manuel Avila Camacho No. 36, Torre Esmeralda II, Piso 7 Com. Lomas de Chapultepec, Guadalajara, Ciudad de Mexico, DF, 11000, Mexico	283804
New Zealand		
Intel New Zealand Limited (LE:930)	c/o Simpson Grierson, 88 Shortland Street, Auckland, 1141, New Zealand	1193185
Peru		
Intel Semiconductores del Peru S.A. (LE:227)	Av. El Derby 254, Piso 25 Office numbers 253, Santiago de Surco, Lima, L33 15023, Peru	11654757
Philippines		
Intel Microelectronics (Phils.) Inc. (LE:880)	Unit 702, 7 th floor, Net3 Cube, 3 rd Ave Corner, 30 th St., E-Square Crescent Park West, Bonifacio Global City, Metro Manila, 1634, Philippines	A1996-07366
Republic of Korea		
Intel Korea Ltd. (LE:800)	4 th Floor, 27-3, Yeouido-dong, Youngdeungpo-ku, Seoul, 150-705, Republic of Korea	110111-0667109
Russian Federation		

AO Intel A/O (LE:450)	17, Krylatskaya str., Bldg. 4, 121614, Moscow, Russian Federation	1027700021470
Intel Technologies LLC (LE:431)	17, Krylatskaya str., Bldg. 4, 121614, Moscow, Russian Federation	1127746104540
Saudi Arabia		
Intel Corporation (UK) Ltd (Saudi Arabia Branch) (LE:456)	Southbound King Fahad Highway, Crossing King Abdullah St. Tatweer Towers, Tower 1 North, Level 4, P.O. Box 246761, Riyadh, 11312, Saudi Arabia	1010172300
Singapore		
Intel Technology Asia Pte Ltd (LE:781)	80 Robinson Road #02-00, 068898, Singapore	199704681N
Intel Foundry Services Pte. Ltd (LE: 798)	9 Raffles Place, #26-01 Republic Plaza, 048619, Singapore	202435713G
South Africa		
Intel South Africa Corp. (Branch) (LE:530)	Office No 265 Design Quarte, Leslie Road, Fourways, Johannesburg, Gauteng, 2191, South Africa	1995/007853/10
Switzerland		
Intel Semiconductor AG (LE:310)	c/o Centralis Switzerland GmbH, Dufourstrasse 101, 8008, Zurich, Switzerland	020.30.913.786-7
Taiwan		

Intel Innovation Technologies Limited (LE:796)	20/F, No.369, Sec 7, Zhong Xiao East Road, NanGang District, Taipei, Taiwan	80510407
Intel Innovation Technologies Limited, Hsinchu Branch (LE:796A)	7F, No. 190, Sec. 2, Zhonghua Road, East Dist., Hsinchu City, Taiwan	53109319
Intel Microelectronics Asia LLC, Taiwan Branch (LE:791)	20/F, No.369, Sec 7, Zhong Xiao East Road, NanGang District, Taipei, Taiwan	16432460

Thailand		
Intel Microelectronics (Thailand) Limited (LE:860)	No. 87, M Thai Tower, All Seasons Place, 23 rd Floor, Unit 2320, Wireless Road, Lumpini Sub-district, Pathumwan District, Bangkok, 10330, Thailand	907/2539
Turkey		
Intel Teknoloji Hizmetleri Limited Sirketi (LE:571)	Hakki Yeten Cad, Selenium Plaza No:10I Kat: 5-6, 34349 Fulya Besiktas, Office 612B, Istanbul, Turkey	799394
United Arab Emirates		
Intel Corporation (UK) Ltd.Dubai Branch (LE:421)	Floor 2, Building 5, Dubai Internet City, Dubai, United Arab Emirates	Lic. No. 20378
Intel R&D UK Ltd – Dubai branch (LE: 457)	Dubai Internet City Building 5, 2nd Floor; Office 207, Dubai, UAE	License # 100766
United Kingdom		
Codeplay Software Ltd. (LE:413)	2 New Bailey, 6 Stanley Street, Salford, Greater Manchester, M3 5GS, United Kingdom	4567874

Intel Corporation (UK) Ltd. (LE:420)	Pipers Way, Swindon, Wiltshire, SN3 1RJ, United Kingdom	1134945
Intel Research and Development UK Ltd (LE:417)	2 New Bailey, 6 Stanley Street, Salford, Greater Manchester, M3 5GS, United Kingdom	13281475
United States		
Digital Content Protection, L.L.C. (LE: 145)	1209 Orange Street, Wilmington DE 19801, United States	3294968
Intel Americas, Inc. (LE:150)	1209 Orange Street, Wilmington DE 19801, United States	FEIN: 77-0521945; DE# 3077423
Intel Capital Corporation (LE:070)	1209 Orange Street, Wilmington DE 19801, United States	DE 2880872 FEIN 77-0498401
Intel Corporation (LE:100)	1209 Orange Street, Wilmington DE 19801, United States	DE 2189074 Tax ID 94-1672743
Intel Czech Tradings, Inc. (LE:475)	818 West 7 th Street, Ste. 930, Los Angeles CA 90017, United States	1828841
Intel Massachusetts, Inc. (LE:113)	1209 Orange Street, Wilmington DE 19801, United States	2822259
Intel Resale Corporation (LE:158)	818 West 7 th Street, Ste. 930, Los Angeles CA 90017, United States	1194886
Intel Semiconductor (US) LLC (LE:760)	1209 Orange Street, Wilmington DE 19801, United States	Tax ID 2666800; EIN 77-0477939
Intel South Africa Corporation (LE:535)	1209 Orange Street, Wilmington DE 19801, United States	2501764
Granulate Cloud Solutions, Inc. (LE: 147)	1209 Orange Street, Wilmington DE 19801, United States	Tax ID 85-1169980

Intel Services Division LLC (LE:036)	1209 Orange Street, Wilmington DE, 19801, United States	EIN 46-4432012
Intel Mobile Communications North America Inc. (LE: 160)	1209 Orange Street, Wilmington DE, 19801, United States	4881018
Habana Labs Inc (LE: 615A)	1209 Orange Street, Wilmington DE, 19801, United States	6323437
Intel Foundry Corporation (LE:101)	1209 Orange Street, Wilmington DE, 19801, United States	4029989
Intel Products IP LLC (LE: 169)	1209 Orange Street, Wilmington DE, 19801, United States	7138713
Vietnam		
Intel Products Vietnam Co., Ltd. (LE:763)	Lot I2, D1 Street, Hi-tech Park, Tan Phu Ward, Thu Duc City, Ho Chi Minh City, Vietnam	0304295429
Intel Vietnam Company Ltd. (LE:766)	Etown Central building, No. 11 Doan Van Bo street, Ward 13, District 4, Ho Chi Minh City, Vietnam	0310516242

APPENDIX 2

FAIR INFORMATION DISCLOSURES

1. Background

1.1 Intel's "Binding Corporate Rules EEA: Controller BCR", the "**Controller BCR**", provides a framework for the transfer of personal data between Intel group members.

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

2. Information to be provided where Intel collects personal data directly from individuals

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

- (a) the **identity and contact details** of the data controller and, where applicable, of its representative;
- (b) the contact details of the **Data Protection Officer**, where applicable;
- (c) the **purposes** of the processing for which the personal data are intended as well as the **legal basis** for the processing;
- (d) where the processing is based on Intel's or a third party's legitimate interests, the **legitimate interests** pursued by Intel or by the third party;
- (e) the **recipients or categories of recipients** of the personal data, if any;
- (f) where applicable, the fact that a group member in Europe intends to **transfer** personal data to a third country or international organization outside Europe, the measures that the group member will take to ensure the personal data remain 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, Intel shall also provide individuals the following further information necessary to ensure fair and transparent processing, at the time of collection:

- (a) the **period** for which the personal data 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 data, to restrict or object to the processing, and 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 data is a **statutory or contractual** requirement or a requirement necessary to enter a contract, whether the individual is obliged to provide the personal data, and the possible consequences of failure to provide such information;
 - (f) the existence of **automated decision-making**, including profiling, and, where such decisions might have a legal effect or significantly affect the individuals whose personal data 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 Intel obtains the personal data from the individual.

3. Information to be provided where Intel collects personal data about individuals from a third-party source

3.1 When Intel collects personal data from a third-party source (that is, someone other than the individual themselves), it must provide the following information:

- (a) the information described in paragraphs 2.1 and 2.2 above;
- (b) the categories of **personal data** that are being processed; and
- (c) **details of the third-party source** from which Intel obtained the personal data including, if applicable, identifying whether the personal data came from publicly accessible sources.

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

- (a) if the personal data are to be used for communication with the individual, the 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 data to another recipient is envisaged, the information described in this paragraph must be provided at the latest when the personal data are first disclosed; in other words, the individual data subject must be informed at or before the time when the individual's personal data are disclosed to third parties.

4. Derogations from providing transparency disclosures

4.1 The requirements to provide 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 proves impossible or would involve a disproportionate effort, and Intel takes appropriate measures, consistent with the requirements of European Union privacy laws, to protect the individual's rights and freedoms and legitimate interests, including by making the information publicly available;
- (c) obtaining or disclosure is expressly laid down by applicable laws to which Intel is subject and these laws provide appropriate measures to protect the individual's legitimate interests; or
- (d) the personal data must remain confidential subject to an obligation of professional secrecy regulated by applicable laws to which Intel is subject, including a statutory obligation of secrecy.

APPENDIX 3

DATA PROTECTION RIGHTS PROCEDURE

1. Background

- 1.1 Intel's "Binding Corporate Rules EEA: Controller BCR" (the "**Controller BCR**") safeguards personal data transferred between the Intel group members.
- 1.2 Individuals whose personal data are processed by Intel under the Controller BCR have certain data protection rights, which they may exercise by making a request to the controller of their information (a "**Data Protection Rights Request**").
- 1.3 This Intel Binding Corporate Rules EEA: Data Protection Rights Procedure ("**Procedure**") describes how Intel will respond to any Data Protection Rights Requests it receives from individuals whose personal data are processed and transferred under the Controller BCR.

2. Individual's data protection rights

- 2.1.1 Intel will enable 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 data about them and, if so, to be provided details of those personal data and access to them. The 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 data a controller might be processing about them. Taking into account the purposes of the processing, the individual shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. 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 data about them, without undue delay, where: i) the personal data are no longer necessary in relation to the purposes for which they were collected or processed, ii) the individual has withdrawn their consent to the processing and there is no other legal ground for processing, iii) the individual objects to the processing and there are no overriding legitimate grounds for

processing or the individual objects to the processing of personal data for direct-marketing purposes, iv) the personal data have been unlawfully processed, v) the personal data have to be erased for compliance with a legal obligation to which the controller is subject, or vi) the personal data have been collected in relation to the offer of information society services to children. Where the controller has made the personal data public and is obliged on request to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, unless this proves impossible or involves disproportionate effort, to inform recipients processing the personal data that the individual has requested the erasure of any links to or copy or replication of those personal data. The controller shall inform the individual about those recipients if the individual requests. 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 data about them where: i) the accuracy of the personal data is contested by the data subject, in which case processing shall be restricted for a period enabling the controller to verify the accuracy of the personal data, ii) the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead, iii) the controller no longer needs the personal data for the purposes of the processing for which they were kept, but the individual requests they be kept for the establishment, exercise, or defense of legal claims, or iv) the individual has objected to processing pursuant to (e) below pending verification of whether the legitimate grounds of the controller override those of the individual. Where processing has been restricted, the personal data shall, with the exception of storage, only be processed with the data subject's consent, for the establishment, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person, or for reasons of important public interest set out in the law of origin of the personal data. A data subject shall be informed by the controller before the restriction of processing is lifted. The controller shall communicate any restriction of processing request to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the individual about those recipients if the individual requests. 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 processing their personal data where such processing is based on the performance of a task carried out in the public interest or the controller's or a third party's legitimate interest. The controller shall no longer process the personal data unless i) the controller demonstrates that compelling, legitimate grounds for the processing override the interests of the individual or ii) for the establishment, exercise, or defense of a legal claim. At any time, an individual may object to the processing of personal data for direct-marketing purposes, which include profiling to the extent that it relates to the direct marketing. Where the individual

objects to processing for direct-marketing purposes, the personal data shall no longer be processed for such purposes. Where personal data are processed for scientific or historical research purposes or statistical purposes, the individual, on grounds relating to their particular situation, shall have the right to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest. 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 data concerning them from a controller in a structured, commonly used and machine-readable format and to transmit that information to another controller where: i) the processing is based on consent or necessity for the performance of a contract, and ii) the processing is carried out by automated means. The process for handling this type of request is described further in paragraph 6 below.

3. Responsibility to respond to a Data Protection Rights Request

3.1 Overview

- 3.1.1 The controller of an individual's personal data is primarily responsible for responding to a Data Protection Rights Request and for enabling the individual concerned to exercise their rights under applicable data protection laws.
- 3.1.2 As such, when an individual contacts Intel to make any Data Protection Rights Request, then, where Intel is the controller of that individual's personal data under the Controller BCR, it must enable the individual to exercise their 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 Intel Privacy Office at <https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html> immediately upon receipt and indicating the date on which it was received together with any other information that might assist the Intel Privacy team to address the request.
- 3.2.2 The Intel Privacy Office will make an initial assessment of the request as follows:
 - (a) the Intel Privacy Office will determine whether Intel is a controller of the personal data that are the subject of the request;
 - (b) where Intel Privacy Office determines that Intel is a controller of the personal data, 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).

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

- (a) If Intel Privacy Office determines that Intel is the controller of the personal data that are the subject of the request, it will contact the individual promptly, and no later than within five (5) working days, in writing (including by email) to confirm receipt of the Data Protection Rights Request.
- (b) A Data Protection Rights Request may be made in writing, which can include email, through Intel's online request form, or orally. A Data Protection Rights Request does not have to be official or mention data protection law to qualify as a valid request.
- (c) Intel will take reasonable steps to verify the identity of the individual making a request and may request such additional information as is necessary for this purpose. Intel may also request further information necessary to address the individual's request.

3.4 *Exemptions to a Data Protection Rights Request*

- (a) Intel will not refuse to act on Data Protection Rights Request unless it can demonstrate that an exemption applies under applicable data protection laws.
- (b) Intel might 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).
- (c) If Intel decides not to take action on the Data Protection Rights Request, Intel will inform the individual without delay and at the latest within one (1) month of receipt of the request of: i) the reasons for not taking action and ii) the right to lodge a claim before the court and a complaint before the competent supervisory authority.

3.5 *Responding to a Data Protection Rights Request*

- (a) Where Intel is the controller of the personal data that are the subject of the Data Protection Rights Request, and Intel 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 Intel shall address the Data Protection Rights Request in accordance with paragraph 4, 5 or 6 below (as appropriate).

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

4. Requests for access to personal data

4.1 Overview

- 4.1.1 An individual may require a controller to provide the following information concerning processing of their personal data:
 - (a) confirmation as to whether the controller holds and is processing personal data about that individual;
 - (b) if so, a description of the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients to whom the information is, or might be, disclosed, the envisaged period(s) (or the criteria used for determining those period(s)) for which the personal data will be stored;
 - (c) information about the individual's right to request rectification or erasure of their personal data or to restrict or object to their processing;
 - (d) information about the individual's right to lodge a complaint with a competent data protection authority;
 - (e) information about the source of the personal data, if they were not collected from the individual;
 - (f) details about whether the personal data are subject to automated decision-making (including automated decision-making based on profiling); and
 - (g) where personal data are transferred outside Europe, the appropriate safeguards that Intel has put in place relating to such transfers in accordance with applicable data protection laws.
- 4.1.2 An individual is also entitled to request a copy of their personal data from the controller. Where an individual makes such a request, the controller must provide to the individual in an intelligible form those personal data to which the individual is entitled.

4.2 Process for responding to access requests from individuals

- 4.2.1 If Intel receives an access request from an individual, this must be passed to the Intel Privacy Office at

<https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html> immediately to make an initial assessment of responsibility consistent with the requirements of paragraph 3.2 above.

- 4.2.2 Where Intel determines it is the controller of the personal data and responsible for responding to the individual directly (and that no exemption to the right of access applies under applicable data protection laws), Intel Privacy Office will arrange a search of the relevant electronic and paper filing systems.
- 4.2.3 The Intel Privacy Office may refer any complex cases to the Data Protection Officer for advice, particularly where the request concerns information relating to third parties or where the release of personal data might prejudice commercial confidentiality or legal proceedings.
- 4.2.4 The personal data that must be disclosed to the individual will be collated by the Intel Privacy Office into a readily understandable format. A cover letter will be prepared by the Intel Privacy Office, which letter will include all information required to be provided in response to an individual's access request (including the information described in paragraph 4.1.1).

4.3 *Exemptions to the right of access*

- 4.3.1 A valid request may be refused on the following grounds:
 - (a) if the refusal to provide the information is consistent with applicable data protection law (for example, where a European group member transfers personal data under the Controller BCR, if the refusal to provide the information is consistent with the applicable data protection law in the European Member State where the group member is located);
 - (b) where the personal data are held by Intel in non-automated form that is not or will not become part of a filing system; or
 - (c) the personal data do not originate from Europe, have not been processed by any European group member, and the provision of the personal data requires Intel to use disproportionate effort.
- 4.3.2 The Intel Privacy Office 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 the Intel Privacy Office.

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

- 5.1 If Intel receives a request to correct, update, erase personal data, or restrict or cease processing of an

individual's personal data, this must be passed to the Intel Privacy Office at <https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html> 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 Intel is the controller of those personal data, the request must be notified to the Intel Privacy Office promptly for it to consider and address as appropriate in accordance with applicable data protection laws.

5.3 When Intel must rectify or erase personal data, Intel will notify other group members and any processor to whom the personal data have been disclosed so that they can also update their records accordingly.

5.4 If Intel acting as controller has made the personal data 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 processing the personal data that the individual has requested the erasure by such controllers of any links to or copy or replication of the personal data.

6. Requests for data portability

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

7. Questions about this Data Protection Rights Procedure

7.1 All queries relating to this Procedure are to be addressed to the Intel Privacy Office or at <https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html>.

APPENDIX 4

PRIVACY COMPLIANCE STRUCTURE

1. Background

1.1 Intel's compliance with global data protection laws and the "Binding Corporate Rules EEA: Controller BCR" (the "**Controller BCR**") is overseen and managed throughout all levels of the business by a global, multi-layered, cross-functional Privacy Compliance Structure.

1.2 Intel's Privacy Compliance Structure has the full support of Intel's executive management. Further information about Intel's Privacy Compliance Structure is set out below.

1.3 For the purposes of this Controller BCR, when a notification is made to Intel Privacy Office such notification shall also be considered to be made to Intel Ireland Limited, since the Intel Privacy Office is a global team.

2. The Privacy Office

2.1 Intel has established a Privacy Office comprised of two primary groups: Privacy Compliance Team (PCT) and Privacy and Security Legal team (PSL) (both privacy-dedicated), supported by additional Intel groups and roles, such as any appointed Data Protection Officers, including the Data Protection Officer for Intel Ireland Limited, Intel Research and Development Ireland Limited, and the Intel legal entities in Germany. This group works together to provide appropriate independence and oversight of duties relating to all aspects of Intel's data protection compliance.

2.2 The Privacy Office is accountable for managing and implementing Intel's data protection program internally (including the Policies) and for establishing effective data privacy controls. In this way, the Privacy Office is actively engaged in addressing matters relating to Intel's data protection compliance on a routine, day-to-day basis. The leadership team of the Privacy Office report out as follows:

- (a) To the Ethics and Compliance Oversight Committee, annually;
- (b) To the Privacy Management Review Committee (Privacy MRC), quarterly. The Privacy MRC oversees implementation of the Privacy Program and is the decision-making body for business unit-level decisions involving privacy compliance risk tolerance.

Any appointed Data Protection Officers will report directly to the highest management level for the companies for which they are appointed and to the Privacy MRC as part of their role in the Privacy Office.

2.3 The Privacy Office's key responsibilities include:

- Defining and communicating the Policies and other data protection related policies, objectives, and standards.
- Evaluating, approving, and prioritizing remedial actions consistent with the requirements of the Policies, strategic plans, business objectives, and regulatory requirements.
- Periodically assessing data protection initiatives, accomplishments, and resources to ensure continued effectiveness and improvement.
- Ensuring that Intel's business objectives align with the Policies and related data protection and information protection strategies, policies, and practices.
- Addressing any escalated data protection complaints in accordance with the Binding Corporate Rules: Complaint Handling Procedure (Appendix 7).
- Supporting the conduct of any data protection audits carried out by supervisory authorities, in accordance with the Intel's Binding Corporate Rules (EEA): Cooperation Procedure (Appendix 8).
- Providing guidance about the collection and use of personal data subject to the Policies and assessing the processing of personal data by Intel group members for potential data protection related risks.
- Responding to inquiries and compliance queries relating to the Policies from workers, customers, and other third parties raised through its dedicated web portal at <https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html>.
- Helping to implement the related policies and practices at a functional and local country level, providing guidance and responding to data protection questions and issues.
- Providing input on audits of the Controller BCR, coordinating responses to audit findings, and responding to inquiries of the supervisory authorities.
- Monitoring changes to global data protection and privacy laws and ensuring that appropriate changes are made to the Controller BCR and Intel's related policies and business practices.
- Overseeing training for workers on the Controller BCR and on data protection legal requirements in accordance with Intel's Binding Corporate Rules (EEA): Privacy Training Program (Appendix 5).
- Promoting the Controller BCR and data protection awareness across business units and functional areas through data protection communications and initiatives.

- Evaluating data protection processes and procedures to ensure that they are sustainable and effective.
- Ensuring that the commitments made by Intel in relation to updating and communicating updates to the Controller BCR are met in accordance with the Intel Binding Corporate Rules (EEA): Updating Procedure (Appendix 9).
- Overseeing compliance with Intel's Binding Corporate Rules (EEA): Data Protection Rights Procedure ([Appendix 3](#)) and the handling of any requests made under it.
- Maintaining a list of all DPOs and their reporting structures and appointment letters.

3. Intel's Chief Privacy Officer (CPO)

Intel's CPO leads the Privacy Office and is responsible for chairing the Privacy MRC, driving Intel's privacy compliance strategy and governance structure, managing Intel's privacy procedures and operational processes, and monitoring the effectiveness of the Privacy Program.

4. Data Protection Officers

Data Protection Officers (DPOs) or other statutorily required roles perform statutory duties at Intel subsidiaries that appoint them to satisfy EU or local law requirements. The DPOs help the Privacy Office make continuous improvements to the operational aspects of the Privacy Program, while performing their statutorily required duties to satisfy local law requirements.

DPOs will not have any tasks that could result in a conflict of interest. DPOs will not be in charge of conducting data protection impact assessments or Controller BCR audits, if such situations can result in a conflict of interest (although they might facilitate/oversee such audits undertaken by an independent auditor).

5. Geographic and Country Privacy Leads

Privacy country and geographic leads have a geographic scope, support the Privacy Office and assist with local data protection law compliance.

6. Business Unit Privacy Leads

The business unit privacy leads and champions are appointed by their business unit and are responsible for helping their business unit comply with the Privacy Program.

7. Intel Workers

7.1 All workers within Intel are responsible for supporting the Privacy Office on a day-to-day basis and adhering to Intel data protection policies.

7.2 In addition, Intel personnel are responsible for escalating and communicating any potential violation of

the data protection policies to the Intel Privacy Office. On receipt of a notification of a potential violation of the data protection policy, the issue will be investigated to determine if an actual violation occurred. Results of such investigations will be documented.

APPENDIX 5

PRIVACY TRAINING PROGRAM

1. Background

- 1.1 The “Binding Corporate Rules EEA: Controller BCR” (“**Controller BCR**”) provide a framework for the transfer of personal data between Intel group members. The document sets out the requirements for Intel to train its workers on the requirements of the Controller BCR.
- 1.2 Intel will annually train its workers on data protection, confidentiality, and information security awareness. This will include training on the Intel Code of Conduct, the Controller BCR, and applicable and relevant data protection laws, including European data protection laws.
- 1.3 Workers who have permanent or regular access to personal data or who are involved in the processing of personal data or in the development of tools to process personal data receive additional, tailored training as described below.

2. Responsibility for the Privacy Training Program

- 2.1 Intel’s Privacy Office has overall responsibility for data protection training at Intel. The Privacy Office will review training from time to time to ensure it addresses the Controller BCR and that it is appropriate for the particular audience.
- 2.2 Intel’s management is committed to the delivery of data protection/privacy training courses and will ensure that relevant workers are required to participate and given appropriate time to complete such courses. Course completion will be measured and reported via regular updates to privacy leadership.
- 2.3 If training audits reveal persistent non-completion, this will be escalated to appropriate managers within Intel who will be responsible and held accountable for ensuring that the individual(s) concerned complete such training.

3. Delivery of the training courses

- 3.1 Intel will deliver data protection training in a variety of ways, including electronic training courses through its on-line learning platform, written materials, recorded content, and in-person sessions. The courses are designed to be both informative and user-friendly, generate interest in the topics covered, and provide appropriate levels of training (dependent on role requirements) to all workers.
- 3.2 Intel’s privacy training content reflects changes in relevant data protection laws and compliance issues arising from time to time.
- 3.3 Certain workers might receive supplemental, specialized training where their business activities include

personal data processing in more unique circumstances (e.g., sales and marketing activities). This specialized training will be tailored as necessary to the course participants.

APPENDIX 6

AUDIT PROTOCOL

1. Background

- 1.1 Intel's "Binding Corporate Rules (EEA): Controller BCR" (the "**Controller BCR**") safeguard personal data transferred between the Intel group members.
- 1.2 Intel will audit its compliance with the Controller BCR on a regular basis, and this document describes how and when Intel will perform such audits. Although this Audit Protocol describes the formal assessment process by which Intel will audit its compliance with the Controller BCR, this is only one way in which the provisions of the Controller BCR are observed and that corrective actions are taken, as required.
- 1.3 In particular, Intel's Privacy Office provides ongoing guidance about the processing of personal data and will continually assess the processing of personal data by group members for potential privacy-related risks and compliance with the Controller BCR.

2. Conduct of an audit

2.1 *Overview of audit requirements*

- 2.1.1 Compliance with the Controller BCR is overseen on a day-to-day basis by the Intel Privacy Office. The Data Protection Officer is responsible for overseeing audits of compliance with the Controller BCR and will design such audits to address all aspects of the Controller BCR. The Data Protection Officer will monitor the reported measurements of compliance provided by the Intel Privacy Office.
- 2.1.2 The Intel Privacy Office or Data Protection Officer will raise any issues or instances of non-compliance with the Controller BCR to legal and operational management so that corrective actions can be determined and implemented within a reasonable time. Serious non-compliance issues will be escalated to Intel's company management (including, where appropriate, Intel's General Counsel, the Ethics and Compliance Oversight Committee, Executive Officers and/or Board of Directors) in accordance with paragraph 2.5.1.

2.2 *Frequency of audit*

- 2.2.1 Audits of compliance with the Controller BCR will be conducted:
 - (a) at least annually in accordance with Intel's audit procedures; and/or
 - (b) at the request of the Ethics and Compliance Oversight Committee, Internal Audit, and/or the Board of Directors; and/or

- (c) as otherwise determined necessary by the Intel Privacy Office or Data Protection Officer (for example, in response to a specific incident).

2.3 *Scope of audit*

- 2.3.1 Audits of compliance with the Controller BCR will verify compliance with all aspects of the BCR by Intel group members (including applications, IT systems, databases that process personal data, onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with this Controller BCR, review of the contractual terms used for transfers outside the Intel group to controllers or processors of personal data, including methods and plans ensuring that corrective actions have been implemented).

The Data Protection Officer, in collaboration with the Intel Privacy Office and any other Intel workers deemed necessary, will determine the scope of an audit following a risk-based analysis, taking into account relevant criteria such as:

- (a) areas of current regulatory focus;
- (b) areas of specific or new risk for the business;
- (c) areas with changes to the systems or processes used to safeguard information;
- (d) use of innovative new tools, systems or technologies;
- (e) areas where there have been previous audit findings or complaints;
- (f) the period since the last review; and
- (g) the nature and location of the personal data processed.

2.4 *Auditors*

- 2.4.1 Audit of the application and implementation of the Controller BCR (including any related procedures and controls) will be undertaken by the Data Protection Officer, in collaboration with the Intel Privacy Office, and other retained internal and external resources as deemed appropriate by the Intel Privacy Office. In addition, Intel may appoint independent and experienced professional auditors, with approval of legal members of the Privacy Office and/or Internal Audit, acting under a duty of confidence and in possession of the required professional qualifications as necessary to perform audits of the Controller BCR (including any related procedures and controls). Intel's Privacy Office will manage and provide quality assurance of audit work performed by others. Intel guarantees the independence of any such auditors as to the performance of their duties related to these audits.

2.5 *Reporting* 2.5.1 Data protection audit reports will be reviewed by senior members of the Intel Privacy Office and shared with Intel Ireland Limited. If the report reveals breaches or the potential for breaches of a serious nature (for example, presenting a risk of potential harm to individuals or to the business), the Intel Privacy Office will escalate these for review by the General Counsel, Ethics and Compliance Oversight Committee, CEO, CIO, and CFO, as appropriate.

2.5.2 Upon request, Intel will provide copies of the results of data protection audits of the Controller BCR (including any related procedures and controls) to the competent supervisory authorities.

2.5.3 The Data Protection Officer is responsible for liaising with the competent supervisory authorities for the purpose of providing the information outlined in paragraph 2.5.2.

2.6 *Supervisory authority audits*

2.6.1 The competent supervisory authorities may audit group members for compliance with the Controller BCR (including any related procedures and controls) in accordance with the Intel Binding Corporate Rules (EEA): Cooperation Procedure ([Appendix 8](#)).

APPENDIX 7

COMPLAINT HANDLING PROCEDURE

1. Background

- 1.1 Intel's "Binding Corporate Rules (EEA): Controller BCR" ("**Controller BCR**") safeguards personal data transferred between the Intel group members.
- 1.2 This Complaint Handling Procedure describes how complaints, questions, enquiries, and concerns ("**complaints**") may be brought by an individual whose personal data are processed by Intel under the Controller BCR will be addressed and resolved.
- 1.3 This procedure will be made available to individuals whose personal data are processed by Intel under the Controller BCR.

2. Enquiries from supervisory authorities

- 2.1 Any enquiry received from a supervisory authority will be immediately referred to the Intel Privacy Office for appropriate action and response in accordance with the Intel Binding Corporate Rules (EEA): Cooperation Procedure ([Appendix 8](#)).

3. How individuals can raise complaints

- 3.1 Any individual may raise a data protection complaint (whether related to the Controller BCR or not) by the following means:

(1) Online at: <https://www.intel.com/content/www/us/en/forms/privacy-contact-us.html>; or

(2) Postal mail to:

Intel Corporation
Attention: Intel Privacy Office
2200 Mission College Boulevard
Santa Clara, CA 95054 USA

OR

Intel Ireland Limited
Attention: Intel Privacy Office
Collinstown Industrial Park
Leixlip
Co. Kildare

3.1.2 Note that Intel workers are also required to direct any privacy-related enquiries and complaints to the Intel Privacy Office in a timely manner.

4. Complaint handling process

4.1 Who handles complaints?

4.1.1 The Intel Privacy Office (which has an appropriate level of independence) will handle all complaints in respect of personal data for which Intel is a controller,

including complaints arising under the Controller BCR. The Intel Privacy Office will liaise with colleagues from relevant business, geography, and support units as necessary to address and resolve complaints.

4.2 What is the response time?

4.2.1 The Intel Privacy Office will acknowledge receipt of a complaint to the individual concerned without undue delay and in any event within five (5) working days of receipt, investigating and making a substantive response within one (1) month.

4.2.2 If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Intel Privacy Office 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.

4.3 What happens if an individual disputes a response given?

4.3.1 If the individual notifies the Intel Privacy Office that they dispute any aspect of the response finding, the Intel Privacy Office will review the case and consult further experts, including relevant Data Protection Officer(s), as required to resolve the concern. The Intel Privacy Office will advise the individual of its decision either to accept or reconsider the original finding within one (1) month from the Intel Privacy Office being notified by the individual that they dispute the response given, provided the timeline will not exceed three (3) months from receiving the initial complaint or request.

4.3.2 If, due to the complexity of the matter, a substantive response cannot be given within one (1) month from the date the individual disputed the response, the Intel Privacy Office 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 individual disputed the response.

4.3.3 If the complaint is upheld, the Intel Privacy Office will arrange for any necessary steps to be taken as a consequence.

5. Right for individuals to complain to a competent supervisory authority and to commence proceedings

5.1 Overview

- 5.1.1 Where individuals' personal data 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 BCR, then those individuals have certain additional rights to pursue effective remedies for their complaints, as described below.
- 5.1.2 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 Intel under this Complaints Handling Procedure. The rights referred to in this paragraph 5.1.2 will also arise where a complaint is rejected by Intel under this Complaints Handling Procedure.
- 5.1.3 Intel accepts 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.

5.2 Complaint to a supervisory authority

- 5.2.1 If an individual wishes to complain about Intel's processing of their personal data to a data protection authority on the basis that a European group member has processed personal data in breach of the Controller BCR or in breach of applicable data protection laws, they may complain about that European group member to the supervisory authority in the European territory:
 - (a) of their habitual residence;
 - (b) of their place of work; or
 - (c) where the alleged infringement occurred.
- 5.2.2 If an individual wishes to complain about Intel's processing of their personal data to a data protection authority on the basis that a non-European group member has processed personal data in breach of the Controller BCR, then, where Part IV of the Controller BCR applies, Intel Ireland Limited will submit to the jurisdiction of the competent supervisory authority (determined in accordance with paragraph 5.2.1 above) in place of that non-European group member, as if the alleged breach had been caused by Intel Ireland Limited.

5.3 Proceedings before a national court

- 5.3.1 If an individual wishes to commence court proceedings against Intel, on the basis that a group member has processed personal data in breach of the Controller BCR or in breach of applicable data protection laws, then they may commence proceedings against that European group member in the European territory:
 - (a) in which that European group member is established; or
 - (b) of their habitual residence.

- 5.3.2 If an individual wishes to commence court proceedings against Intel on the basis that a non-European group member has processed personal data in breach of the Controller BCR, then, where Part IV of the Controller BCR applies, Intel Ireland Limited will submit to the jurisdiction of the competent court (determined in accordance with paragraph 5.3.1 above) in place of that non-European group member, as if the alleged breach had been caused by Intel Ireland Limited.

APPENDIX 8

CO-OPERATION PROCEDURE

1. Background

- 1.1 Intel's Binding Corporate Rules (EEA): Cooperation Procedure sets out the way in which Intel will cooperate with competent supervisory authorities in relation to the "Intel Binding Corporate Rules (EEA): Controller BCR" ("**Controller BCR**").

2. Cooperation Procedure with Supervisory authorities

- 2.1 Where required, Intel will make the necessary personnel available for dialogue with a competent supervisory authority in relation to the Controller BCR.
- 2.2 Intel Privacy Office will review, consider, take into account, and comply with:
- (a) any advice or decisions of relevant competent supervisory authorities on any data protection law issues that might affect the Controller BCR; and
 - (b) any guidance published by supervisory authorities (including the European Data Protection Board or any successor to it) in connection with Binding Corporate Rules for Controllers.
- 2.3 Intel Privacy Office will provide upon request copies of the results of any audit it conducts of the Controller BCR to a competent supervisory authority.
- 2.4 Intel agrees that a competent supervisory authority may audit or inspect, including, where necessary, on-site, any group member for compliance with the Controller BCR.
- 2.5 Intel agrees to abide by a formal decision of any competent supervisory authority on any issues relating to the interpretation and application of the Controller BCR (unless and to the extent that Intel is entitled to appeal any such decision and has chosen to exercise such right of appeal).
- 2.6 Intel agrees, upon request, to provide the relevant, competent supervisory authority any information about the processing operations covered by this Controller BCR.
- 2.7 Any dispute related to the competent supervisory authorities' exercise of supervision of compliance with the Controller BCR will be resolved by the courts of the Member State of that competent supervisory authority, in accordance with that Member State's procedural law. Each group member agrees to submit themselves to the jurisdiction of these courts.

2. Cooperation Procedure between Group Members

- 2.1 Group members will cooperate and assist each other and the Intel Privacy Office when handling requests or complaints regarding the Controller BCR from individuals and/or company supervisory authorities.
- 2.2 Group Members will comply with any instructions from Intel Ireland Limited or Intel Corporation requiring a remedy of a breach of the Controller BCR.

APPENDIX 9

UPDATING PROCEDURE

1. Background

- 1.1 Intel's Binding Corporate Rules (EEA): Updating Procedure describes how Intel will communicate changes to the "Binding Corporate Rules (EEA): Controller BCR" ("**Controller BCR**") to competent supervisory authorities, individual data subjects, and Intel group members bound by the Controller BCR.
- 1.2 Any reference to Intel in this procedure is to the Intel Privacy Office, which is accountable for ensuring that the commitments made by Intel in this Updating Procedure are met.

2. Record keeping

- 2.1 Intel will maintain a change log that sets out details of each revision made to the Controller BCR, including the nature of the revision, the reasons for making the revision, the date the revision was made, and who authorized the revision.
- 2.2 Intel must also maintain an accurate and up-to-date list of group members that are bound by the Controller BCR.
- 2.3 The Intel Privacy Office shall be responsible for ensuring that the records described in this paragraph 2 are maintained and kept accurate and up-to-date.

3. Changes to the Controller BCR

- 3.1 All proposed changes to the Controller BCR must be reviewed and approved by the Intel Privacy Office, so that a high standard of protection is maintained for the data protection rights of individuals who benefit from the Controller BCR. No changes to the Controller BCR shall take effect unless reviewed and approved by the Intel Privacy Office.
- 3.2 Intel Privacy Office will communicate all changes to the Controller BCR (including reasons that justify the changes) to:
 - (a) the group members bound by the Controller BCR via written notice (which may include e-mail or posting on an internal Intranet accessible to all group members) without undue delay;
 - (b) individuals who benefit from the Controller BCR via online publication at www.intel.com; and
 - (c) the supervisory authority that was the lead authority for the purposes of granting Intel's BCR authorization ("**Lead Authority**") and any other relevant supervisory authorities the Lead

Authority may direct, at least once a year. The Lead Authority should also be notified once per year in instances where no changes have been made.

4. Communication of material changes

4.1 If Intel makes any material changes to the Controller BCR or to the list of group members bound by the Controller BCR that affect the level of protection offered by the Controller BCR or otherwise significantly affect the Controller BCR (for example, by making changes to the binding nature of the Controller BCR), it will promptly report such changes (including the reasons that justify such changes) to the Lead Authority and all group members.

5. Transfers to new group members

5.1 If Intel intends to transfer personal data to any new group members under the Controller BCR, it must first ensure that all such new group members are bound by the Controller BCR before transferring personal data to them.

APPENDIX 10

GOVERNMENT DATA REQUEST RESPONSE PROCEDURE

1. Background

- 1.1 Intel's Binding Corporate Rules (EEA): Government Data Request Response Procedure sets out Intel's Procedure for responding to a request received from a law enforcement authority or state security body (together the "**Requesting Authority**") to disclose personal data processed by Intel (hereafter "**Data Disclosure Request**"). This procedure also applies when Intel becomes aware of any direct access by public authorities to personal data transferred pursuant to this Controller BCR in accordance with the laws of the country of destination.
- 1.2 Where Intel 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 data than is required by this Procedure, Intel 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, Intel does not disclose personal data in response to a Data Disclosure Request unless either:
- (a) it is under a compelling legal obligation to make such disclosure (such as a Court order or a statutory duty to make 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.

3. Handling of a Data Disclosure Request

3.1 *Receipt of a Data Disclosure Request*

- 3.1.1 If an Intel group member receives a Data Disclosure Request, the recipient of the request must pass it to Intel's Privacy Office immediately upon receipt, indicating the date on which it was received together with any other information that might assist Intel's Privacy Office to handle 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, however made, must be notified to the Intel Privacy Office for review.

3.2 *Initial steps*

3.2.1 The Intel Privacy Office will carefully review each and every Data Disclosure Request on a case-by-case basis and address 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 might be needed to challenge the Data Disclosure Request.

3.2.2 Intel will refer to and apply any specific procedures that it has established to govern the process by which further engagement takes place (for example, how to identify whether a compelling, legal Data Disclosure Request has been made). Any such procedures shall be consistent with the requirements of this Government Data Request Response Procedure.

4. Notice of a Data Disclosure Request

4.1 Where a group member outside Europe receives a legally binding request by a public authority under the laws of the country of destination or of another third country for disclosure of personal data or becomes aware of any direct access by public authorities to personal data transferred pursuant to this Controller BCR, it will promptly inform:

4.1.1 the data exporter;

4.1.2 the Privacy Office (and the Privacy Office shall inform Intel Ireland Limited), and

4.1.3 the individual(s) (where possible).

The notice should include details of the personal data requested, the Requesting Authority, the legal basis for the disclosure, and the response provided.

4.2 Where Intel is prohibited from notifying the data exporter and/or the individual(s) and suspending the request, Intel 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 might include asking the Requesting Authority to put the request on hold or seeking a court order to this effect. Intel will maintain a written record of the efforts it takes.

4.3 The data importer will provide the data exporter, at regular intervals, as much relevant information as possible on the requests received (in particular, the number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged, and the outcome of such challenges). If the data importer is or becomes partially or completely prohibited from providing the data exporter this information, it will, without undue delay, inform the data exporter accordingly.

- 4.4 The data importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by this Controller BCR and will make it available to the competent supervisory authorities upon request.

5. Challenge to request

- 5.1 The data importer agrees to review, under the laws of the country of destination, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.
- 5.2 The data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer will seek interim measures with a view to suspend the effects of the request until the competent judicial authority has decided the challenge on the merits. The data importer will not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the data importer pursuant to Part I of this Controller BCR (i.e., the obligation to notify the Intel Privacy Office if it has reason to believe it cannot comply with this Controller BCR).
- 5.3 The data importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It will also make it available to the competent supervisory authorities upon request.

6. Transparency reports

- 6.1 Intel 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. Intel shall provide this report to the lead supervisory authority that authorized the Controller BCR (and any other supervisory authorities that the Lead Authority may direct) once a year.

7. Bulk transfers, data minimization

- 7.1 Intel shall not transfer personal data to a Requesting Authority in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

APPENDIX 11

MATERIAL SCOPE OF THE CONTROLLER BCR

1. Background

1.1 Intel's "Binding Corporate Rules EEA: Controller BCR" (the "**Controller BCR**") provides a framework for the transfer of personal data between Intel group members.

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

2. Human Resources Data

Who transfers the personal data described in this section?	Every Intel group member inside Europe may transfer the personal data that they control and are described in this section to every Intel group member outside Europe.
Who receives the personal data?	Every Intel group member outside Europe may receive the personal data described in this section that are transferred to them by Intel group members inside Europe.
What categories of personal data are transferred and who are the types of individuals whose personal data are transferred?	i. Candidates: name, contact details, employment history, qualifications, education, and references. ii. Employees: details collected in relation to the recruitment process (see above), performance data (including promotion information, performance management data, disciplinary information), financial data (bank details for payment of salary, bonus, and benefits), medical information (limited to what is necessary to provide reasonable accommodations), emergency contact details, details of beneficiaries and dependants (benefits-administration required data), personal data collected from the employees' use of Intel's assets (e.g., use of Intel mobile phones, calls made, use of Intel resources, transmission of data on Intel devices, etc.), and information submitted voluntarily by employees (e.g., in the context of employee surveys aimed at improving diversity and inclusion at Intel). iii. Independent Contractors: name, contact details, education background, occupational history, government-issued identification or other identification numbers, physical location, information about the contingent worker's employer (e.g., the agency supplying them), time worked (e.g., hours or days) for compensation purposes, contingent worker's preferred contact in case of emergency, or identification or travel profile data if business travel is required, and use of Intel assets (where applicable), which category might include identifying hardware data, network connection information, IP

	address and geographic location (such as through GPS, Bluetooth, or WiFi signals). iv. Ex-Employees: details collected during employment, termination reasons, asset return, post-termination contact details (if different to during employment). v. Ex-Independent Contractors: certain details collected during the term of their engagement with Intel, termination reasons, and details on Intel asset return. v. Non-employee-related data: Beneficiary data (e.g., names, dates of birth) for life assurance benefits (where provided); name, date of birth, email address for the provision of healthcare benefits (where added to employees' policy); details to be found in the policy documents for the relevant service.
--	---

Are categories of sensitive personal data transferred?	Medical information might be transferred if such information is necessary to provide reasonable accommodations for an individual employee or independent contractor. Other categories of sensitive personal data might be transferred, depending on an individual situation, such as information in relation to disciplinary actions, background checks (where permitted by law) or (if submitted voluntarily by employees, e.g., in the context of an employee survey on diversity and inclusion) information on racial or ethnic origin or sexual orientation.
Why are the personal data transferred and how will they be used?	Why are the personal data transferred? All group members have access to employee directory information (including names, job title, contact information, and skills) to collaborate on projects across geographic borders; group members support each other with respect to hiring, mentoring, and professional development across borders; managers access performance and development information regarding employees of other group members as necessary for human resources and talent management purposes; group members assist each other with respect to technology and administrative resources to optimize payroll and benefits administration. How will the personal data be used? • Candidates: Recruitment and hiring, including interviewing, assessing suitability for permanent or temporary employment, making travel arrangements (where applicable), background checking (to the extent permitted under law), and hiring processes. • Employees: Managing the employment relationship, including delivery of applicable compensation and benefits programs; human resources practices, including on-boarding, promotion, retention, and discipline; centralizing and processing human resources

	information; participation in company-provided programs and events; career development opportunities; promotion of healthy lifestyles and an inclusive working environment (e.g., free from discrimination on grounds of sex, sexual orientation, racial or ethnic origin, or disability); assurance of a safe (e.g., protect against physical or digital security threats) working environment, and legal obligations (e.g., investigating violations of law of company policy, responding to legal warrants or discovery processes), including notifying family members or designated contacts in case of emergency; assessing suitability for employment or particular position. • Independent Contractors: Managing the contractual relationship with contingent workers, including documenting Statements of Work or similar orders; onboarding that includes completion of forms and issuance of assets, processing compensation, engaging with the worker during the assignment, assurance of a safe working environment (e.g., protect against physical or digital security threats), and legal obligations (e.g., investigating violations of law of company policy, responding to legal warrants or discovery processes), including notifying family members or designated contacts in case of emergency, and business-travel related processing. • Ex-Employees: Post-termination processing, including off-boarding, transfer of benefits provision, meeting legal and compliance obligations (e.g., relating to data retention periods). • Non-employee Data: Provision of services and benefits (e.g., to dependents and family members); emergency contact in case of injury/death of an employee.
Where are the personal data processed?	The personal data described in this section may be processed in every territory where Intel group members or their processors (meaning processors that are also members of the Intel group) are located. A list of Intel group member locations is available at: https://www.intel.com/content/www/us/en/location/worldwide.html.

3. Customer Relationship Management Data

Who transfers the personal data described in this section?	Every Intel group member inside Europe may transfer the personal data that they control and are described in this section to every Intel group member outside Europe.
Who receives the personal data?	Every Intel group member outside Europe may receive the personal data described in this section that are transferred to them by Intel group members inside Europe.

What categories of personal data are transferred and who are the types of individuals whose personal data are transferred?	i. General customer information: name, contact details, and, where relevant, bank account information. ii. Newsletter subscribers, account creator, and information requestors: name, contact details, and feedback or preferences. iii. Social media users: information from third-party operating sites or services to which Intel links; information provided by app developers or providers, social media platform providers, operating system provider, wireless service provider, or device manufacturers, including any personal data that data subject discloses to other organizations through or in connection with the relevant Intel services or Intel social media pages. iv. Research, analysis, and study participants: name, contact details, data subject input into the study/research, feedback, or preferences. v. Sweepstakes, contests, and similar promotions participants: name, contact details. vi. Recipients of advertising and marketing materials: name, contact details, times of visits by device and traffic sources, actions made by the device owner, device owner's interests, and other data used to provide enhanced functionality and personalization. vii. Web page visitors: IP address, location of device, times of visits by device, traffic sources, actions made by the device owner, device owner's interests, and other data used to provide enhanced functionality and personalization (according to user preferences).
--	--

Are categories of sensitive personal data transferred?	The following types of sensitive personal data will be transferred from time to time: • Social media users: any sensitive information a user decides to disclose during their use of social media. • Research analysis and study participants: depending on the focus area of a research project, sensitive data might be transferred.
--	--

Why are the personal data transferred and how will they be used?	Why are the personal data transferred? Intel is a globally operating company, with customers located in different parts of the world. In order to support Intel's global operations, Intel has employees, business units, and company functions located at different, international Intel sites. Personal data need to be transferred internationally, so that employees working in different business units and/or in different company functions can have access to the personal data required to complete assigned tasks, to collaborate with colleagues located at different international sites, and to generally keep Intel's businesses running. How will the personal data be used? • Provide goods or services to the customer and perform related tasks, such as product delivery; to send messages; to ship products and process payments; to respond to customer service requests; to provide alerts such as security updates or changes in our policies or about subscriptions that are ending; and to send marketing or informational materials like newsletters or white papers, in accordance with data subject communication preferences. • In order to allow for social-media interaction and content sharing. • Conduct research, analysis, historical and scientific studies either alone or with partners, e.g., surveys, or focused research or studies. • Conduct sweepstakes, contests, and similar promotions. • Enable joint products or research studies, or to facilitate services like message boards, blogs, or other shared platforms. • To enable personalized content and to study the effectiveness of advertising and marketing campaigns. • To improve user experience, by providing visitors personalized content and remembering preferences.
Where are the personal data processed?	The personal data described in this section might be processed in any territory where Intel group members or their processors (meaning processors that are also members of the Intel group) are located. A list of Intel group member locations is available at: https://www.intel.com/content/www/us/en/location/worldwide.html.

4. Supply Chain Management Data

Who transfers the personal data described in this section?	Every Intel group member inside Europe may transfer the personal data that they control and are described in this section to every Intel group member outside Europe.
--	--

Who receives the personal data?	Every Intel group member outside Europe may receive the personal data described in this section that are transferred to them by Intel group members inside Europe.
What categories of personal data are transferred and who are the types of individuals whose personal data are transferred?	The following personal data are collected from individual contractors, account managers, and workers of third-party suppliers to Intel: • business contact information (name, job title, email, and phone number); • skills and Intel procurement history; and • information described above at no. 3 (iii) & (v) might also be collected from individual contractors, depending on the services being provided to Intel.
What categories of sensitive personal data (if any) are transferred?	Medical information might be transferred if such information is necessary to provide reasonable accommodations for an individual contractor. Other categories of sensitive personal data might be transferred, depending on an individual situation, such as information in relation to background checks on individual contractors (where permitted by law).
Why are the personal data transferred and how will they be used?	Business contact information is required for every engagement to facilitate transactions. Specific personal data are transferred for defined business needs as specified in the procurement agreement (e.g., HR data transferred to payroll processors to provide services required to calculate and pay compensation to individual contractors) or participant/customer data to support sales/marketing events and transactions.
Where are the personal data processed?	The personal data described in this section might be processed in any territory where Intel group members or their processors (meaning processors that are also members of the Intel group) are located. A list of Intel group member locations is available at: https://www.intel.com/content/www/us/en/location/worldwide.html .