DATA PROTECTION POLICY

This Data Protection Policy ("**Policy**") of InterDigital, Inc. and its wholly owned subsidiaries (collectively, "**InterDigital**" or the "**Company**") establishes the standards and compliance rules that all InterDigital employees, officers, directors, contractors, vendors, outsourced service providers, representatives, and agents (collectively, "**Personnel**") must follow regarding the protection of Personal Data handled by the company regarding natural persons, including without limitation customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact ("**Data Subjects**").

The primary goal of this Policy is to provide for compliance with applicable data protection laws with respect to InterDigital's business operations.

A secondary goal of this Policy is to reinforce other policies relating to the collection, use, handling, retention or maintenance of information which includes Personal Data, as per the InterDigital Records Management Policy, Information Security Policy, Physical Security Policy, and Incident Response Policy (collectively, "**Company Policies**") by setting a high standard of respect of privacy of natural persons by the company.

A tertiary goal is to reinforce the InterDigital Incident Response Policy relating to the reporting, escalation or remediation of security incidents, such as a data breach.

Compliance with this Policy and Company Policies is of the highest importance to the Company.

1. Introduction:

The Company needs to gather and use certain information about data subjects. . This Policy describes how Personal Data must be collected, handled or stored to meet the company's data protection standards, and to comply with applicable laws.

This Policy ensures that the Company:

- Complies with data protection laws and follows good business practices with respect to data protection, handling, and storage;
- Protects the rights of its Personnel with respect to Personal Data;
- Is as transparent as is necessary and required to appropriately store and Process data from data subjects;
- Protects itself from the risk of a data breach of Personal Data.

2. Definitions

- "**Data Protection and Privacy Laws**" means, collectively any applicable data protection and privacy laws and administrative rules which regulate the Processing of Personal Data by or on behalf of the Company. Data Protection and Privacy Laws include without limitation the General Data Protection Regulation in force in the European Union, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any other applicable state laws.
- **"Data Regulator"** means any local, state, national or multinational agency, department, governmental body, regulatory or supervisory authority, board or other public body responsible for administering the Data Protection and Privacy Laws. "Data Regulator" includes without limitation any "Supervisory Authority" under Data Protection and Privacy Laws.
- **"Data Subject"** means an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or other information. Data Subject or Consumers includes all "data subject" as defined by Data Protection and Privacy Laws.
- **"Data Subject Rights"** means certain rights provided to Data Subjects under Data Protection and Privacy Laws, and under the conditions of such Data Protection and Privacy Laws, including the right to:
- Withdraw consent at any time;

- Request information about why and how Personal Data is being Processed and disclosed by the Company;
- Request the deletion of Personal Data
- Request access to their Personal Data
- Receive a copy of their Personal Data
- Correct Personal Data that would be incorrect
- Object to or restrict Processing of their Personal Data;
- Receive their Personal Data in a portable format;
- Request information about how the Company is meeting its data protection obligations;
- Terminate any sales or sharing of their Personal Data
- Be informed that the Data Subject may have a right to file a complaint with a Data Regulator.
-
- **"Personal Data"** means any information that identifies, relates to, describes, is capable of being associated with, or could be linked to, directly or indirectly, a Data Subject, including Personnel. "Personal Data" includes without limitation name; personal or business address, email address, telephone number; date of birth; gender; marital status; emergency contacts; nationality or work entitlement; bank details; social insurance information; tax identification information; employment agreements; salary and benefits information; hours and days of work; leave periods or basis for leave; qualifications and skills; work experience; employment history; disciplinary or grievance record; performance reviews and related correspondence; or equal opportunities monitoring information. "Personal Data" also includes all "personal data," "personal information" and all other information that is regulated under Data Protection and Privacy Laws.
- **"Personal Data Breach"** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed. "Personal Data Breach" includes all "Personal Data breach," "breach of security," or other breach of Personal Data under any other Data Protection and Privacy Laws;
- "**Processing**," "**Process**," and "**Processed**" mean any creation, access, modification, disclosure, transfer, storage, deletion, destruction, or other use of Personal Data. "Processing" includes all "Processing" as defined in Data Protection and Privacy Laws.
- "**Sensitive Personal Data**" means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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. "Sensitive Personal Data" includes all "sensitive data," "sensitive personal information," or "special categories of Personal Data" under Data Protection and Privacy Laws.

3. Authorities and Responsibilities

This Policy is approved by InterDigital's Chief Legal Officer. Responsibility for implementation and continued management and improvement is delegated as follows:

- The Chief Legal Officer is responsible for: (a) ensuring that agreements entered by the Company address the requirements defined in this Policy, as appropriate; and (b) communicating those requirements to third parties where they exist.
- The Chief Information Security Officer is responsible for implementation of controls and Processes for IT infrastructure, security planning, management, improvement and reporting.
- The head of Human Resources is responsible for ensuring all employees acknowledge and are trained on the requirements of this Policy.
- Managers are responsible for ensuring that their direct reports comply with the requirements of this Policy.
- All Personnel are responsible for ensuring that they comply with the requirements of this Policy.

4. Policy Acknowledgement

All Personnel shall review this Policy and acknowledge their review and compliance upon hire and as requested by the company from time to time. Annual or periodic training regarding this Policy may be required.

5. Data Protection and Privacy Laws

Data Protection and Privacy Laws apply regardless of whether data is stored electronically, on paper, or on other materials or media. To comply with Data Protection and Privacy Laws, Personal Data must be (i) collected and used fairly, lawfully and in a transparent manner; (ii) collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes; (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed; (iv) accurate and, where necessary, kept up to date; (v) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed; and (vi) Processed and stored using reasonable technical and organizational measures design to avoid any Personal Data Breach.

6. Security

Reasonable security measures must be taken. In the unlikely event that a Personal Data Breach occurs, an investigation shall be conducted and further steps shall be taken as deemed by the Company to be reasonably necessary under the circumstances.

All Personnel are instructed to ***immediately*** report any actual or suspected Personal Data Breach to Company Legal using the email address Privacy@InterDigital.com, or by contacting Olivier LE QUERE (Olivier.lequere@interdigital.com).

7. General Guidelines

These general guidelines are intended to supplement, but not supersede, the guidelines provided in the InterDigital Information Security Manual (*see* Section 18, Data Security) and Physical Security Policy:

- Personnel should collect, access and use Personal Data only when it is legally approved. In case of doubt, before collecting, accessing or using Personal Data, guidance from InterDigital Legal should be requested.
- Personnel should keep all Personal Data secure, by taking reasonable precautions such as by using strong passwords and only storing Personal Data in authorized locations on the network.
- The only Personnel with access to Personal Data, as covered by this Policy, should be those who require access to it to complete their assigned work and or fulfill their duties for the company.
- Personal Data should not be shared informally, and when access to Personal Data is required, Personnel must request it from their supervisors.
- Personal Data should not be disclosed to unauthorized persons, either within the company or externally.
- Where applicable, Personal Data should be regularly reviewed and updated if it is found to be out of date. If no longer needed, it should be destroyed in accordance with the Records Management Policy.
- The Company will provide training to all Personnel to help them understand their responsibilities when handling Personal Data.
- Personnel should request assistance from their supervisor or Legal if they are unsure about any aspect of data protection for Personal Data.

8. Data Storage

Information regarding how to safely store and manage Personal Data can be found in Company Policies, and any questions about how to safely store Personal Data can be directed to the IT Department.

- When Personal Data is stored on paper, it should be kept in a secure place where unauthorized Personnel or third parties cannot access or view it.
- This Policy also applies to Personal Data that is usually stored electronically but has been made into a hard copy; accordingly,
    - When not required, the paper or files should be kept in a locked space, drawer or filing cabinet;
    - Personnel should make sure paper and printouts are not left where unauthorized Personnel or third parties could see them, such as laying unattended on a printer;

    - Printouts of Personal Data, which are duplicative of electronic files, should be shredded and securely disposed of when no longer needed; and,
    - Personnel should take any other reasonable actions to protect Personal Data which has been made into a hard copy and should seek assistance from a manager or IT Personnel with any questions.
- When Personal Data is stored electronically, it must be protected from unauthorized internal and external access, accidental deletion and unauthorized modification. To mitigate this risk,
    - Personal Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services using secure methods of transmission;
    - Personal Data should be held in as few places as necessary and Personnel should not unnecessarily create or store any additional sets of Personal Data;
    - If Personal Data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used, and, where reasonably practicable, the Personal Data on the removable media should be encrypted;
    - Avoid saving Personal Data directly to local drives on laptops or other mobile devices like tablets or smart phones, and, where reasonably practicable, the Personal Data on such mobile devices should be encrypted, including through the use of whole disk encryption;
    - Personnel should take any other reasonable actions to protect Personal Data under the circumstances and should seek assistance from a manager or IT Personnel with any questions; and
    - When Personal Data is Sensitive Personal Data, additional security measures may be required, as recommended by Legal or IT such as maintaining logs of any access to Sensitive Personal Data, protection by enhanced password requirements, or restrictions on where Sensitive Personal Data can be stored.

9. Data Subject Requests

Data Subject who are the subject of Personal Data held by the Company may exercise the Data Subject Rights.

If such an individual contacts the Company requesting to exercise a Data Subject Right, it is called a "**Data Subject Request**." Data Subject Requests from such individuals shall be made using standard forms which are publicly available on Company websites. In response to a Data Subject Request pursuant to Data Protection and Privacy Laws, InterDigital may be subject to response deadlines. In accordance with applicable laws, the required response times begin after InterDigital had been able to verify the identity of the person making a Data Subject Request. The Company will review the request in consideration of any other applicable regulations and laws of the relevant jurisdiction and respond by the deadline and in the manner required by Data Protection and Privacy Laws.

Accordingly, Personnel receiving a Data Subject Request from a third party are <u>not</u> authorized or permitted to directly respond to such requests. All Data Subject Requests shall be forwarded to InterDigital Legal, and will be handled by InterDigital Legal.

Personnel are instructed to ***immediately*** provide the Data Subject Request, and any and all relevant information relating to the Data Subject Request, to InterDigital Legal for review and handling.

10. Process (Law Enforcement or Legal Process) Access Requests

In certain circumstances, Data Protection and Privacy Laws allow Personal Data to be disclosed to law enforcement agencies without the consent of the Data Subject. If such a disclosure is requested, it is called a "**Process Access Request**." In response to a Process Access Request, InterDigital may be subject to response deadlines. Under these circumstances, InterDigital may disclose such Personal Data which is subject to these requests. InterDigital will endeavor to respond, as appropriate, within required time periods after (a) verifying the legitimacy of the Process Access Request, and (b) reviewing the request in consideration of any other applicable regulations and laws of the relevant jurisdiction.

Accordingly, Personnel receiving a Process Access Request from a third party are <u>not</u> authorized or permitted to directly respond to such requests. All responses to Process Access Requests shall be forwarded to InterDigital Legal, and will be handled by InterDigital Legal.

Personnel are instructed to ***immediately*** provide the Process Access Request, and any and all relevant information relating to the Process Access Request, to InterDigital Legal for review and handling and are required to implement instructions given by the Company in this respect.

12. Data Retention

Unless if retention is required by applicable law, InterDigital shall ensure that Personal Data are not kept for longer than is reasonably necessary for the purpose for which the Personal Data is collected.

Retention periods take into account:

- The purpose for which the Personal Data was collected or subsequent purpose that would be lawfully admissible;
- any legal, professional rules of conduct or obligations under applicable laws to retain Personal Data for a certain period of time (for example in relation to tax, health and safety, and employment laws);
- any contractual obligations to retain Personal Data;
- the Company's need to deal with any disputes or potential disputes, including anticipated or actual litigation or regulatory proceedings; and
- guidelines issued by any relevant regulatory authorities, including Data Regulators;
- the generally accepted best practices of the legal industry or of the applicable affiliate of the Company receiving Personal Data.

InterDigital destroys, in a secure manner, Personal Data which it no longer needs to keep in accordance with this Policy; provided that, InterDigital may anonymize information in a manner compliant with Data Protection and Privacy Laws, so that Data Subjects, including its Personnel, cannot be identified.

Accordingly, Personnel are instructed to comply with the above-stated principles and to ***immediately*** cease Processing Personal Data where required thereby.

13. Transfers of Personal Data

InterDigital will not transfer Personal Data to any third party, country or territory, unless InterDigital and the recipient take reasonable and appropriate steps designed to ensure Personal Data is Processed securely and in accordance with this Policy the Company Policies, and Data Protection and Privacy Laws.

InterDigital will only export Personal Data to countries deemed to provide adequate privacy protection by the European Commission ("Adequate Countries") or to countries where additional safeguards can be used to provide equivalent protection in compliance with Data Protection and Privacy Laws ("Other Countries"). Personal Data transferred to Other Countries will be subject to specific safeguards, compliant with Data Protection and Privacy Laws, provided under a Data Transfer Agreement entered by and between InterDigital International, Inc. and its affiliates or between the Company and a subconctractor which would have a need-to-know these information.

The Company may disclose Personal Information to "Service Providers", "Contractors", and "third parties" (each as defined by the CCPA) and/or to a third Party acting as "Processor" as defined in GDPR for the purposes defined in section "**Lawful basis for Processing Personal Data**" of the notice (the Purpose).

"Service Providers", "Contractors" and "Processors" are third parties that process Personal Data that we provide or make available in connection with a written contract that includes certain Data Privacy Laws-required restrictions, such as prohibiting the sale of Personal Information or disclosing Personal Information other than as permitted in our contract with the Service Provider. A "Third Party" is a third party that receives Personal Data from us for any other purpose.

When the Company discloses Personal Data for the Purpose, we enter into an agreement with the receiving party that describes the purpose for sharing the Personal Data, and that requires the receiving party to keep that Personal Data confidential. In the case of disclosures to our Service Providers, our Service Providers are obligated not to use the Personal Information for any purpose other than performing the services according to their agreement with us. In the case of our Contractors, our Contractors are obligated not to use the Personal Information for any purpose unrelated to the business purpose for which we've engaged them.

If Personnel would like more information about the safeguards that are used to protect their Personal Data when it is Processed outside the European Economic Area ("EEA") and to implement it, they may contact InterDigital Legal using the email address Privacy@InterDigital.com, or by contacting Olivier LE QUERE (Olivier.lequere@interdigital.com)

14. Exceptions, Confidentiality, and Administration

Exceptions:

Requests for exceptions from this Policy should be submitted to the Legal Department for review and approval.

If an exception is initiated, the affected persons will be notified. Once it is determined that an exception is no longer required, Legal will terminate the exception and re-initiate application of the Policy with respect to the affected persons. This decision will be appropriately documented. For the avoidance of doubt, any exception granted cannot and will not supersede the compliance with Data Protection and Privacy Laws.

Confidentiality:

This Policy is confidential and proprietary to InterDigital and is not to be distributed outside of InterDigital without written approval of InterDigital's Legal Department.

Administration:

InterDigital's Legal Department has overall responsibility for creating and interpreting this Policy. Each individual is responsible for ensuring that the procedures identified in this Policy are effected in accordance with its requirements.

Review and Updates:

This Policy is subject to change. Requirements under this Policy shall be periodically reviewed to ensure that it reflects current legal and business practices and requirements. Any changes to the Policy based upon new or revised regulatory or operational requirements must be reviewed and approved by the Legal Department.

Effective Date: March 1, 2023

1. INTERDIGITAL, INC. - PRIVACY NOTICE TO INTERDIGITAL PERSONNEL

This Privacy Notice ("Notice") is provided to explain how InterDigital, Inc., including its wholly owned subsidiaries ("InterDigital," "we," "us," "our"), handles and uses Personal Data that is collected regarding its personnel worldwide ("you" or "your") and your rights in connection with our use of your Personal Data.

This Notice is part of the InterDigital Data Protection Policy ("Policy"). Any capitalized terms not defined in this Notice shall have the meaning assigned to them in the Policy. This Notice and the Policy may be updated from time to time to reflect changes in laws and regulations relating to the use of Personal Data and other changes in our Processing of your Personal Data. Where changes pertain to the Processing of your data we will notify you of the changes.

. If you have questions regarding this Notice, you should either submit them to Legal (olivier.lequere@interdigital.com), or the general EU Privacy email address at Privacy@InterDigital.com.

Why we hold your Personal Data

We collect and Process your Personal Data for the purposes listed below. We use Personal Data:

- for human resources management (for example, recruitment, career development, training, social benefits, talent management, performance management, appraisals and disciplinary and grievance management);
- for staff administration and operational purposes (for example, in relation to absences, pay, benefits, compensation, stock administration, business travel, maintaining employee directories, enabling access to our systems and resources, managing authorization controls, ensuring the security of our systems and resources, management forecasts and planning changes in our group structure);
- to appropriately file and prosecute applications for patents, trademarks and copyrights in all countries as selected by InterDigital;
- for detecting or preventing any inappropriate behavior or breach of our policies including protecting our intellectual property, confidential information and assets;
- for making contact in an emergency;
- for ensuring that our (or any of our group companies) systems are used primarily for business purposes, have sufficient capacity for the needs of the business, are protected against cybersecurity threats such as malware;
- for the purposes of any potential and/ or actual litigation or investigations concerning us or any group company or its officers; and
- to carry out, where necessary and permitted by law, appropriate criminal record and background screening checks, including with respect to education.

Types of Personal Data

The Personal Data we hold regarding you include information such as:

- Name.
- Personal and business address.
- Personal and business email address.
- Personal and business telephone number.
- Employee ID
- Date of birth.
- Gender.
- Marital status.

- Children (age, gender)
- Emergency contacts.
- Your nationality and entitlement to work in areas that requires you to have a specific title to work.
- Passport information
- Bank details.
- Tax identification number, national insurance number, social information system number and other government-issued identifier
- Your employment contract(s) (including all information related to it such as your status, job, title, grade, domain, supervisor, date of employment, date of end of your contract, reason of the end of your contract).
- Salary and benefits.
- Your hours and days of work.
- Details of periods of leave taken by you, such as holiday, sickness, maternity/paternity leave or other leave and the reasons.
- Qualifications and skills.
- Work experience and employment history.
- Your disciplinary or grievance records.
- Performance reviews and related correspondence.
- Equal opportunities monitoring information.
- Tax information when locally required.

We may also collect Sensitive Personal Data as further provided below:

Employees and candidates for employment:

- Racial or ethnic origin (if and where needed for equal opportunity monitoring information as per applicable law)
- Sexual orientation (if and where needed for equal opportunity monitoring information as per applicable law)
- Health information that you would voluntarily provide and that are required to grant you some specific rights (for example, disability that would grant you the right to specific equipment provided by InterDigital or to work under a specific organization). InterDigital does not require that you provide such information if you do not feel comfortable doing so and will not collect or Process this information unless directly provided by you.
- Trade union membership (if and where needed for equal opportunity monitoring information or adjustment of employee's work -ie time given for union work- as per applicable law)
- Equal opportunities monitoring information (if and where needed for equal opportunity monitoring information as per applicable law) Social Security, driver's license, state identification card, or passport number;
- Account log-in, financial account, debit card or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- the contents of mail, email, and text messages unless, with respect to information relating to California residents, the Company is the intended recipient of the communication.

Such Sensitive Personal Data will be collected and Processed:

- with your consent, unless another legal basis applies, and only as permitted by Data Protection and Privacy Laws.
- They are needed for a legitimate goal such as for equal opportunities monitoring and/or where such information is needed to enforce local regulation.
- The Sensitive Personal Data collected will be as limited as possible considering the aimed goal.

For instance, union membership will be collected in France to implement local union regulation, while no racial or ethnic origin or sexual orientation will be collected in France as required by local regulations.

Collection of Personal Data

We collect your Personal Data in a variety of ways. When possible, we collect the data that you directly provide including without limitation using:

- Application forms, CVs or resumes;
- Your passport or other identity documents, such as your driving license;
- Forms completed by you at the start of, or during, your employment or engagement with us (such as employment agreements or benefit forms);
- Correspondence with you; and
- Interviews, meetings or other assessments.

We may from time to time collect information that we lawfully receive from third Party such as:

- Government agencies (such as the IRS or similar tax administration, social security services);
- Employment agencies, when applicable; and
- Landlord of your work building (for instance, using the access control log from the doors of your building).
- licensing organizations,
- benefits providers, insurers,
- our payroll provider with respect to Employees, including documents required for employment or tax reporting information required by us as an employer.

Lawful basis for Processing Personal Data

There are several reasons why we hold, Process and share individuals' Personal Data. Under Data Protection and Privacy Laws, the lawful reasons for Processing Personal Data include:

- For the performance of a contract. *We need to Process Personal Data to enter into an employment contract or other contract of engagement with you and to meet our obligations under such contract. For example, we need to Process your Personal Data to provide you with a contract, to pay you in accordance with your contract or to administer benefit or other employment related entitlements. If you do not provide this Personal Data, we may be unable in some circumstances to comply with our obligations or may not be able to employ you.*
- To comply with a legal obligation. *In some cases, we need to Process Personal Data to ensure that we are complying with our legal obligations. For example, we must check an employee's or worker's entitlement to work in a specific country, deduct tax, comply with health and safety laws and enable staff to take periods of leave to which they are entitled. In some cases, we need to Process your Personal Data in order to comply with legal obligations, a court order, or the order of a governmental authority outside of the EU.*
- To protect the vital interests of the individual or another person, or a task carried out in the public interest. *This legal basis can be used where, for example, we need to disclose information about you to prevent you or someone else from being seriously harmed or killed. An example can include providing information to a medical professional about you in circumstances where you are unable, physically or legally, to provide the information yourself. It may cover an emergency situation.*
- For a legitimate interest except where those rights are overridden by the interests or fundamental rights and freedoms of the data subject which require protection. *We Process your Personal Data for the purposes listed below as part of our legitimate interest in the efficient management of our workforce, defense of legal claims and cooperation with investigation.*
    - Operate and keep a record of employee performance and related Processes, to plan for career development, and for succession planning and workforce management purposes.

- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
- Obtain occupational health advice, to ensure that we comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organization complies with contractual or legal duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- Operate and keep a record of disciplinary and grievance Processes, to ensure acceptable conduct within the workplace.
- Respond to and defend against legal claims or other investigatory Processes.
- Perform a contract that we may hold with a third party such as with a third-party service provider for cloud-based storage.

In certain circumstances, we may only lawfully Process your Personal Data with your consent. Where this is the case we will request your consent before we Process your Personal Data for that purpose. If you have given your consent to anything we do with your Personal Data, you have the right to withdraw your consent at any time (although if you do so, it does not mean that anything we have done with your Personal Data with your consent up to that point is unlawful and we may not be able to carry out the activity for which we obtained your consent).

How we share your Personal Data

Other members of staff: We share your Personal Data with other members of staff in order for them to perform their roles. This can include sharing Personal Data with the senior leadership team, Human Resources, Legal, your manager, other managers and IT staff on a need-to-know basis.

Amongst the InterDigital entities: We will disclose Personal Data about you between and among various InterDigital companies for the management of the employment or service relationship, grant of benefits, patent filings, management of budget and related purposes.

Third party service providers: We also share your data with third parties that Process data on our behalf, which include, but are not limited to companies such as ADP, Etrade, and/or WorkDay in connection with payroll, the provision of benefits and occupational health services, or Unicom in connection with the prosecution of patent applications. Throughout these Processes, we maintain strict confidentiality and only Process and retain the Personal Data in accordance with our Records Management Policy and the Processing purposes stated above. Such transfer is subject to the prior execution of a Data Transfer Agreement executed with this provider with provision at least as protective as this policy.

Research institutions: We may also share your Personal Data) with third parties in a consulting or research agreement with a third-party research institution if you are the company representative.

Compliance with legal obligations: We will share your Personal Data as necessary to order to comply with legal obligations, a court order, or the order of a regulatory authority, in the jurisdictions in which we operate, including under US Federal and state laws. The legal basis for such sharing of your information is within our legitimate interest in the efficient administration of our workforce, in carrying our business and in compliance with legal obligations.

Business reorganization: If we are involved in a business reorganization, such as a merger or a sale of our assets or in a dissolution, liquidation or bankruptcy proceedings (including in negotiations toward such transaction or in the course of proceedings), we may be required to share information about our employees in connection with such a transaction or proceeding.

Sending information to other countries

In order to administer certain aspects of your employment relationship, we transfer your Personal Data outside the European Economic Area (EEA), respectively, to our headquarters in the United States or to service providers who are located in the United States. To carry out this transfer in accordance with the requirements of EU data protection

laws, InterDigital entities have entered into a data transfer agreement incorporating Standard Contractual Clauses approved by the EU Commission.

Protecting Personal Data

We take the protection of your Personal Data very seriously. We have implemented and maintain internal policies and controls to reasonably ensure that data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by employees with a need to know such information for the performance of their duties. For additional information on how we protect your Personal Data and company proprietary information, please refer to the InterDigital Information Security Policy, Physical Security Policy, and Incident Response Policy.

Where we engage third parties to Process Personal Data on our behalf, they do so based upon written instructions, under a duty of confidentiality and with an obligation to implement appropriate technical and organizational measures to ensure the security of data. For example, we use encrypted devices, strong passwords, virus protection and appropriate firewalls, and we have a full suite of IT policies to ensure protection of systems and personnel.

Automated decision-making and profiling

We do not make automatic decisions or undertake automated decisions regarding individuals to evaluate certain information about an individual (profiling).

Retention of Personal Data

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected, and for the time during which we may need it to assert legal claims or defend against claims. We will also retain Personal Data as required by applicable legal obligations.

Your rights

You have the following rights:

To be informed	This Notice provides the information you are entitled to receive. You will also be informed of an Personal Data Breach impacting your Personal Data as soon as we become aware of such breach.
Access	Please contact Legal if you would like confirmation that your data is being Processed, and Human Resources for access to your Personal Data, *e.g.*, in your personnel file. There is no charge for us providing you with this information and a response will usually be provided within a month of the request (unless the request is unfounded or excessive).
Rectification	Please inform us of any Personal Data which you would like rectified, *e.g.*, in your personnel file. We will review and respond within a month of the request. Where appropriate, we will pass on the changes to any third parties who need to change their records and let you know this has been done.
Erasure	You may exercise your right to have your Personal Data erased in a number of circumstances. We will comply with all such requests, subject to applicable laws and regulations.
To object	Please submit objections to the Processing of your Personal Data to Legal. We will review and respond within a month of the request.
Data Portability	You may request the transfer of certain of your personal information to another party.

If you would like to exercise any of the above rights, we ask that you raise your concern with us in the first instance by contacting Legal at Olivier.lequere@interdigital or Human Resources .

Further guidance and advice on the above rights can be obtained from the local privacy authority (such as CNIL in France or Information Commissioner's Office in UK).

Complaints

If you have a concern about the way we are collecting or using your Personal Data, we ask that you raise your concern with us in the first instance by contacting your direct supervisor, and/or Legal Olivier.lequere@interdigital.com or Human Resources.

You also have a right to lodge a complaint with a supervisory authority, in particular in the Member State in the European Union where you are habitually resident, where you work or where an alleged infringement of data protection laws has taken place. In France, you can make a complaint to the French data protection authority (the *Commission Nationale de l'Informatique et des Libertés*) (Tel: 01 53 73 22 22 or at www.cnil.fr). In England you can make a complaint to the Information Commissioner's Office (ICO) https://ico.org.uk/make-a-complaint/.

Effective Date: March 1, 2023

PRIVACY NOTICE TO CALIFORNIA PERSONNEL

This Privacy Notice to California Personnel (this "Notice") is part of the InterDigital Data Protection Policy ("Policy"). Any capitalized terms not defined in this Notice shall have the meaning assigned to them in the Policy. This Notice and the Policy may be updated from time to time to reflect changes in laws and regulations relating to the use of Personal Data and other changes in our Processing of your Personal Data. Where changes pertain to the Processing of your data we will notify you of the changes.

The Company has adopted this Notice to comply with the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and their implementing regulations (collectively, the "**CCPA**").

This Notice applies solely to prospective, current and former job applicants, employees and contractors of the Company (each, as applicable, a "**Role**") who are residents of the State of California (each, an "**Employee,**" "**You,**" or "**Your**") and to Related Individuals (as defined below) who are residents of the State of California. This Notice describes the collection, use, disclosure, and destruction of Your Personal Information (as defined in Section 1 below) by the Company in connection with Your Role. This Notice also applies to Personal Information about other individuals that You provide to the Company in connection with the Company's administration of Your Role, such as Personal Information about Your emergency contacts or, if applicable, participants or beneficiaries of Your employee benefits (collectively, "**Related Individuals**").

1. INFORMATION THE COMPANY COLLECTS

The Company collects Personal Data, including Personal Data about You or a Related Individual ("**Personal Information**"). In particular, the following categories of Personal Information may have been collected from or about You by or on behalf of the Company within the last twelve (12) months:

- Name.
- Personal and business address.
- Personal and business email address.
- Personal and business telephone number.
- Employee ID
- Date of birth.
- Gender.
- Marital status.
- Children (age, gender)
- Emergency contacts.
- Your nationality and entitlement to work in areas that requires you to have a specific title to work.
- Passport information
- Bank details.
- Tax identification number, national insurance number, social information system number and other government-issued identifier
- Your employment contract(s) (including all information related to it such as your status, job, title, grade, domain, supervisor, date of employment, date of end of your contract, reason of the end of your contract).
- Salary and benefits.
- Your hours and days of work.
- Details of periods of leave taken by you, such as holiday, sickness, maternity/paternity leave or other leave and the reasons.
- Qualifications and skills.
- Work experience and employment history.
- Your disciplinary or grievance records.
- Performance reviews and related correspondence.
- Equal opportunities monitoring information.
- Tax information when locally required.

We also may collect Sensitive Personal Information. "**Sensitive Personal Information**" means Personal Information that is not publicly available and reveals one or more of the following:

Employees and candidates for employment:

- Racial or ethnic origin (if and where needed for equal opportunity monitoring information as per applicable law)
- Sexual orientation (if and where needed for equal opportunity monitoring information as per applicable law)
- Health information that you would voluntarily provide and that are required to grant you some specific rights (for example, disability that would grant you the right to specific equipment provided by InterDigital or to work under a specific organization). InterDigital **does not** require that you provide such information if you do not feel comfortable doing so and will not collect or Process this information unless directly provided by you.
- Trade union membership (if and where needed for equal opportunity monitoring information or adjustment of employee's work -ie time given for union work- as per applicable law)
- Equal opportunities monitoring information (if and where needed for equal opportunity monitoring information as per applicable law) Social Security, driver's license, state identification card, or passport number;
- Account log-in, financial account, debit card or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- the contents of mail, email, and text messages unless the Company is the intended recipient of the communication.

Such Sensitive Personal Data will be collected and Processed:

- with your consent, unless another legal basis applies, and only as permitted by Data Protection and Privacy Laws.
- They are needed for a legitimate goal such as for equal opportunities monitoring and/or where such information is needed to enforce local regulation.
- The Sensitive Personal Data collected will be as limited as possible considering the aimed goal.

Personal Information does not include:

- publicly available information from government records;
- information that we have a reasonable basis to believe is lawfully made available to the general public by You or from widely distributed media;
- information made available by a person to whom You disclosed such information without restriction;
- de-identified or aggregated information; and
- information excluded from the CCPA's scope, such as:
    - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
    - Personal Information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

We collect your Personal Data in a variety of ways. When possible, we collect the data that you directly provide including without limitation using:

- Application forms, CVs or resumes;
- Your passport or other identity documents, such as your driving license;

- Forms completed by you at the start of, or during, your employment or engagement with us (such as employment agreements or benefit forms);
- Correspondence with you; and
- Interviews, meetings or other assessments.

We may from time to time collect information that we lawfully receive from third Party such as:

- Government agencies (such as the IRS or similar tax administration, social security services);
- Employment agencies, when applicable; and
- Landlord of your work building (for instance, using the access control log from the doors of your building).
- licensing organizations,
- benefits providers, insurers,
- our payroll provider with respect to Employees, including documents required for employment or tax reporting information required by us as an employer.

2. USE OR DISCLOSURE OF PERSONAL INFORMATION

There are several reasons why we hold, Process and share individuals' Personal Data. Under Data Protection and Privacy Laws, the lawful reasons for Processing Personal Data include:

- For the performance of a contract. *We need to Process Personal Data to enter into an employment contract or other contract of engagement with you and to meet our obligations under such contract. For example, we need to Process your Personal Data to provide you with a contract, to pay you in accordance with your contract or to administer benefit or other employment related entitlements. If you do not provide this Personal Data, we may be unable in some circumstances to comply with our obligations or may not be able to employ you.*
- To comply with a legal obligation. *In some cases, we need to Process Personal Data to ensure that we are complying with our legal obligations. For example, we must check an employee's or worker's entitlement to work in a specific country, deduct tax, comply with health and safety laws and enable staff to take periods of leave to which they are entitled. In some cases, we need to Process your Personal Data in order to comply with legal obligations, a court order, or the order of a governmental authority outside of the EU.*
- To protect the vital interests of the individual or another person, or a task carried out in the public interest. *This legal basis can be used where, for example, we need to disclose information about you to prevent you or someone else from being seriously harmed or killed. An example can include providing information to a medical professional about you in circumstances where you are unable, physically or legally, to provide the information yourself. It may cover an emergency situation.*
- For a legitimate interest except where those rights are overridden by the interests or fundamental rights and freedoms of the data subject which require protection. *We Process your Personal Data for the purposes listed below as part of our legitimate interest in the efficient management of our workforce, defense of legal claims and cooperation with investigation.*
    - Operate and keep a record of employee performance and related Processes, to plan for career development, and for succession planning and workforce management purposes.
    - Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
    - Obtain occupational health advice, to ensure that we comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
    - Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organization complies with contractual or legal duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.

    - Operate and keep a record of disciplinary and grievance Processes, to ensure acceptable conduct within the workplace.
    - Respond to and defend against legal claims or other investigatory Processes.
    - Perform a contract that we may hold with a third party such as with a third-party service provider for cloud-based storage.
- as described to You when collecting Your Personal Information and as otherwise required or permitted under the CCPA.

Additionally, the Company may use or disclose Sensitive Personal Information for one or more of the following purposes:

- to fulfill or meet the reason You provided the information, including to provide or administer employment benefits or to evaluate equal employment opportunity compliance;
- to respond to law enforcement requests and as required by applicable law, court order, or governmental regulations;
- to respond to Your requests under the CCPA;
- for any other purpose described to You when we collect Your Sensitive Personal Information; and
- for any other permissible or acceptable purposes as set forth in the CCPA.

InterDigital will not transfer Personal Data to any third party, country or territory, unless InterDigital and the recipient take reasonable and appropriate steps designed to ensure Personal Data is Processed securely and in accordance with this Policy the Company Policies, and Data Protection and Privacy Laws.

InterDigital will only export Personal Data to countries deemed to provide adequate privacy protection by the European Commission ("Adequate Countries") or to countries where additional safeguards can be used to provide equivalent protection in compliance with Data Protection and Privacy Laws ("Other Countries"). Personal Data transferred to Other Countries will be subject to specific safeguards, compliant with Data Protection and Privacy Laws, provided under a Data Transfer Agreement entered by and between InterDigital International, Inc. and its affiliates or between the Company and a subconctractor which would have a need-to-know these information.

The Company may disclose Personal Information to "Service Providers", "Contractors", and "third parties" (each as defined by the CCPA) and/or to a third Party acting as "Processor" as defined in GDPR for the purposes defined in section "Lawful basis for Processing Personal Data" of the notice (the Purpose).

"Service Providers", "Contractors" and "Processors" are third parties that process Personal Data that we provide or make available in connection with a written contract that includes certain Data Privacy Laws-required restrictions, such as prohibiting the sale of Personal Information or disclosing Personal Information other than as permitted in our contract with the Service Provider. A "Third Party" is a third party that receives Personal Data from us for any other purpose.

When the Company discloses Personal Data for the Purpose, we enter into an agreement with the receiving party that describes the purpose for sharing the Personal Data, and that requires the receiving party to keep that Personal Data confidential. In the case of disclosures to our Service Providers, our Service Providers are obligated not to use the Personal Information for any purpose other than performing the services according to their agreement with us. In the case of our Contractors, our Contractors are obligated not to use the Personal Information for any purpose unrelated to the business purpose for which we've engaged them. We may disclose Your Personal Information with the following categories of entities:

Categories of Personal Information	Business Purpose	Types of Recipients
Name, address, social security number of You and your spouse/domestic partners and any dependents; birth date; medical condition; compensation information	Provision and administration of benefits programs, including health insurance, leave benefits and retirement plans	Health, disability and leave insurers and/or administrators, and third-party providers handling the Company's 401(k) plans
Name, address, social security number, compensation information	Payroll and tax reporting	Payroll provider, federal, state and local tax authorities
Name, address, compensation information; racial or ethnic origin, religious or philosophical beliefs, and any other status protected by applicable anti-discrimination laws; performance evaluations; discipline	Compliance with subpoenas and/or governmental requests; preparation of affirmative action plans; compensation reviews	Governmental entities, parties to pending litigation and/or their attorneys

3. Sales and Sharing of Personal Information

"**Sell,**" "**Selling,**" "**Sale,**" or "**Sold**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Information to another business or a third party for monetary or other valuable consideration.

"**Share,**" "**Sharing,**" or "**Shared**" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Information to a third party for Cross-context Behavioral Advertising, whether or not for monetary or other valuable consideration.

"**Cross-context Behavioral Advertising**" means the targeting of advertising to an individual based on that individual's Personal Information obtained from activity across businesses or distinctly-branded websites, applications, or services, other than the business or distinctly-branded website, application, or service with which the individual intentionally interacts.

We do not Sell or Share Your Personal Information. We will not Sell or Share Your Personal Information without providing notice to You and getting Your consent.

4. Retention and Deletion of Personal Information

Unless retention is required by applicable law, InterDigital shall ensure that Personal Data are not kept for longer than is reasonably necessary for the purpose for which the Personal Data is collected.

Retention periods take into account:

- The purpose for which the Personal Data was collected or subsequent purpose that would be lawfully admissible;
- any legal, professional rules of conduct or obligations under applicable laws to retain Personal Data for a certain period of time (for example in relation to tax, health and safety, and employment laws);
- any contractual obligations to retain Personal Data;
- the Company's need to deal with any disputes or potential disputes, including anticipated or actual litigation or regulatory proceedings; and
- guidelines issued by any relevant regulatory authorities, including Data Regulators;
- the generally accepted best practices of the legal industry or of the applicable affiliate of the Company receiving Personal Data.

InterDigital destroys, in a secure manner, Personal Data which it no longer needs to keep in accordance with this Policy; provided that, InterDigital may anonymize information in a manner compliant with Data Protection and Privacy Laws, so that Data Subjects, including its Personnel, cannot be identified.

Accordingly, Personnel are instructed to comply with the above-stated principles and to ***immediately*** cease Processing Personal Data where required thereby.

5. Your Rights and Choices

You may request information about our collection, use, disclosure and Sale of Your Personal Information, whether or not it was collected electronically. For purposes of this Section 5, You includes Related Individuals.

"**Verifiable Request**" means that the identifying information You provide in connection with a request matches the Personal Information the Company already maintains. Identifying information includes Your name, address, and date of application or date of hire.

If You submit a Verifiable Request, you may require the following rights:

- Withdraw consent at any time regarding data collection;
- Request information about why and how Personal Data is being Processed and disclosed by the Company;
- Request the deletion of Personal Data
- Request access to their Personal Data
- Receive a xcopy of their Personal Data
- Correct Personal Data that would be incorrect
- Object to or restrict Processing of their Personal Data;
- Receive their Personal Data in a portable format;
- Request information about how the Company is meeting its data protection obligations;
- Terminate any sales or sharing of their Personal Data.

We may deny Your deletion request if retaining Your Personal Information is necessary for us or our Service Providers or Contractors to:

- complete a transaction for which we collected Your Personal Information, provide goods or services that You requested, take actions reasonably anticipated within the context of Your ongoing Role with us or otherwise to perform a contract between us or in connection with the Personal Information of a Related Individual;
- help ensure security and integrity, including to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- debug services, products and websites to identify and repair errors that impair existing intended functionality;
- exercise free speech, ensure the right of another consumer to exercise their right of free speech, or exercise another right provided for by law;
- comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.);
- engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the achievement of such research, if You previously provided informed consent;
- enable solely internal uses that are reasonably aligned with the expectations of Employees based on Your Role with us; or
- comply with a legal obligation.

You also have the right to request that we limit the use and disclosure of Sensitive Personal Information by submitting a Verifiable Request. If You submit such a Verifiable Request, we may continue to use or disclose Your Sensitive Personal Information to:

- complete a transaction for which we collected Your Sensitive Personal Information, provide goods or services that You requested, take actions reasonably anticipated within the context of our ongoing business relationship with You, or otherwise perform our contract with You;
- detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- use in a short-term and transient manner, including, but not limited to, to facilitate non-personalized advertising shown as part of Your current interaction with the technologies used by the Company, but not including disclosure to third parties or use outside Your current interaction with such technologies;
- enable solely internal uses that are reasonably aligned with employee expectations based on Your relationship with us; or
- make any other uses of that information that are permitted by the CCPA and its implementing regulations.

If You choose to exercise a privacy right under the CCPA, You have the right not to receive discriminatory treatment.

You may submit a Verifiable Request for the information listed above, or exercise any of Your rights enumerated under this Notice, by calling us at [PHONE NUMBER], or by completing a form on our website, or by email to Olivier.lequere@interdigital. You may also submit a Verifiable Request on behalf of Your minor child.

After we receive Your Verifiable Request to access or receive a copy of your Personal Information, we will provide to You, in writing and free of charge (unless Your request is excessive, repetitive, or manifestly unfounded), the requested information. Unless you specify a shorter period for the request, and so long as processing Your request does not require disproportionate effort, we will process Your request to access or receive a copy of Personal Information we have collected from January 1, 2022 to the time of processing your request. You can choose to have this information delivered to You by postal mail or electronically. We will try to respond to Your verified request within forty-five (45) days of receipt, but if we require more time (up to another forty-five (45) days) we will inform You of the reason and extension period in writing. Please note that we are not required to comply with Your request for information more than twice in any 12-month period. If applicable, our response will explain the reasons why we cannot comply with Your request.

The Company does not and will not, without first obtaining Your consent, Sell or Share Personal Information.

If You choose to exercise any of the rights enumerated under this Notice, we will not:

- deny You goods or services;
- charge You different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties;
- provide You a different level or quality of goods or services; or
- suggest that You may receive a different price or rate for goods or services or a different level or quality of goods or services.

However, please be aware that it is necessary for the Company to have Personal Information about You in order for You to be employed by the Company and for us to provide You with Employee benefits. Additionally, it may be a functional necessity for us and/or our technologies to have Personal Information about You in order to operate, and we may not be able to provide some or all of our benefits or services to You if You direct us to delete Your Personal Information.

6. Changes to this Notice

We may amend this Notice from time to time. When we make changes to this Notice, we will notify You through by email or on an internal Company website.

7. Contact Information

If You have any questions or comments about this Notice, the ways in which we collection, use, disclosure, or destroy Your Personal Information, Your choices and rights regarding Your Personal Information, please do not hesitate to contact us at Olivier.lequere@interdigital.