OpenAI Global Data Privacy Notice for Employees, Applicants and Candidates
Last updated: April 23, 2026

This Global Data Privacy Notice ("Data Privacy Notice") describes how OpenAI OpCo, LLC and its subsidiaries/affiliates (collectively, "OpenAI") collect, use, disclose, store, and otherwise process personal data in the context of job candidacy, employment or engagement with OpenAI. This Data Privacy Notice includes additional information for specific jurisdictions, available in the Addenda located here: EEA/UK/Switzerland; U.S./Canada; Japan; Korea, Singapore; Australia; India; United Arab Emirates (ADGM); and Brazil.

We hold and process data on all current and former employees, workers, individual contractors, contingent workers, applicants, interview candidates, interns, agency workers, consultants, directors, members (i.e. partners) (**"staff"** or **"you"** or **"your"**), and third parties whose information you provide to us in connection with a job application or the employment or other working relationship.

The OpenAI entity to which you submit an application for employment or with which you are providing services for (which we'll refer to throughout this notice as the "Company," "we," "our," or "us") is responsible for the processing of your personal data. Purely for the purposes of this Data Privacy Notice, references to employment include engagement where you do work for us and you are not an employee.

This Data Privacy Notice does not form part of any contract of employment or engagement you may have with the Company. We may undertake certain processing of personal data that is subject to additional or separate data privacy notice, and we shall bring these to your attention where relevant. If you have any questions about this Privacy Notice, or would like to access the information it contains in a different format please contact us at hr@openai.com.

OpenAI's processing of personal data is in all cases subject to the requirements of applicable local law, internal policy, and where applicable or appropriate, any consultation requirements with worker representatives. To the extent this notice conflicts with local law in your jurisdictions, local law controls.

For further information regarding your rights as described in this Notice, or to exercise any of your rights, please contact us at hrprivacy@openai.com.

1.0 Processing of Personal Data

The Company collects and processes your personal data for the purposes described in this Notice. Personal data means any information describing or relating to an identified or identifiable individual, or as otherwise defined in applicable law. An identifiable individual 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 individual.

We collect various types of personal data about you for the purposes described elsewhere in this Data Privacy Notice. Data that we may collect from or about you (depending on the specifics of your employment or engagement, your office location, or the time you spend at OpenAI) may include:

Personal details	Such as your name(s), , gender, nationality(ies), civil / marital status, date of birth, age, contact details, social security number, immigration / eligibility to work information, driver's license, languages spoken, next-of-kin / dependent / emergency contact information, disability / reasonable adjustments information;
Information about your r**ecruitment and hire**	Such as skills and experience, qualifications, references, CV and application, information collected during the recruitment and interview process, results of credit reference check, financial sanction check and criminal record check if permitted by applicable law, right to work verification, outcome of your application, details of any offer made;
Information about your **employment and engagement**	Such as your contract/terms of employment or engagement, work contact, employee or payroll number, photograph, work location default hours, default language, time zone and currency for location, worker ID and system IDs, work biography, assigned business unit or group, reporting line, employment type (e.g., contingent worker/employee, full/part time), your hire/contract begin and end dates, cost center, working hours and patterns, reason(s) for a change in work status, exit interviews, references provided, and status (active/inactive/terminated). If you are subject to a redundancy or restructuring, we may collect information related to this including change plans, organization charts, consultation records, and selection and redeployment data;
Regulatory data	Such as records of registration with any applicable regulatory authority, regulated status, regulatory certificates and references;
Information related to your **compensation and benefits**	Such as your remuneration information, payments for leave/absence, bank account details, grade, tax information, benefit recipient information, details of available benefits, benefit coverage start and end date, expense claims and payments, loans, deductions, salary sacrifice arrangements, childcare vouchers, and share scheme information (including for staff in Germany: church tax code);
Information about a **leave or absence**	If you go on leave (such as family leave, or other types of leave such as bereavement leave, jury service, or compassionate leave) or otherwise take a term of absence while at OpenAI, we may collect information such as attendance and absence records (including dates and types of absence and relevant approvals). To the extent required by law, we may also collect other information about a specific type of leave of absence, including fit notes details of incapacity, work impact and adjustments, treatment and prognosis, manager and HR

	communications, return to work interviews, meeting records, medical reports, occupational health reports;
Information about f**lexible working procedure**	Such as requests, consideration, correspondence, meeting notes and outcome records;
Information related to your **job performance**	Such as feedback, appraisals, and performance management and review information, outcomes and objectives, talent program assessments and records, succession plans;
Information about your **training and development**	Such as training and development needs, training received, and assessments completed;
Information about **disciplinary actions and grievances**	Such as allegations, complaints, investigations, and proceeding records and outcomes;
Health and safety data (as applicable)	Such as health and safety audits, screening requests and results, risk assessments, incident reports;
Information related to your **use of our offices, company devices, and other company assets**	Such as data generated from monitoring and management of company assets (e.g., closed circuit television footage, system and building login and access records including badge swipes, keystroke, download and print records, information about calls or meetings, data caught by IT security programs and filters);
Information about **employee claims, complaints and disclosures**	Such as subject matter of litigation and complaints, pre-claim conciliation, communications, settlement discussions, claim proceeding records, incident reporting and disclosures. This also may include personal data related to OpenAI's (or a third parties') establishment, exercise and/or defense of rights generally; personal data required to comply with applicable law, or personal data relating to responses to law enforcement or government requests;
Equality and diversity data	Such as, where permitted by law and provided voluntarily, data regarding gender, age, race, nationality, religious belief and/or sexuality (which we treat as need-to-know and use, for example, to comply with federal contractor regulations where applicable);

Other	Such as any other personal data you choose to disclose verbally or in writing to Company personnel during the course of recruitment or your engagement; informal opinion data generated in the course of recruitment or your engagement relating to the administration or management of the Company's relationship with you. This may include, for instance, information relating to the conduct of OpenAI's business, including carrying out roles and responsibilities, communications with colleagues and business partners, and internal reporting. Certain additional information will sometimes be collected where this is necessary and permitted by local applicable laws.

SENSITIVE DATA

To the extent permitted by applicable laws, and with your consent where required by applicable law, we may collect sensitive personal data (sometimes called special categories of personal data). This term means information relating to: racial or ethnic origin; political opinions; religious or philosophical beliefs; physical or mental health (including details of accommodations or adjustments); trade union membership; sex life or sexual orientation; biometric and genetic data; criminal records and information regarding criminal offenses or proceedings; financial information; or as otherwise defined by applicable data protection laws.

2.0 HOW IS DATA COLLECTED

The Company collects and records your personal data from a variety of sources, but mainly directly from you, and where required by applicable law, with your consent. You will usually provide this information directly to your managers or local Human Resources contact or enter it into our systems (for example, through your self-service access to our HR systems, your participation in HR processes, emails, Slack, and instant messages you send or through verbal information which may be recorded electronically or manually). In addition, further information about you will come from your managers or Human Resources or occasionally your colleagues.

We also obtain some information from third parties: for example, references from a previous employer, medical reports from external professionals, information from tax authorities, benefit providers, where we employ a third party to carry out a background check (where permitted by applicable law), business partners, and government agencies and authorities as well as social insurance providers.

In some circumstances, data will sometimes be collected indirectly from monitoring devices or by other means (for example, building and location access control and monitoring systems, CCTV, telephone logs and recordings, instant message logs and email and Internet access logs), if and to the extent permitted by applicable laws. In these circumstances, the data may be collected by the Company or a third-party provider of the relevant service. This type of data is generally not accessed on a routine basis but access is possible. Access can occur, for instance, in situations where OpenAI is investigating possible violations of Company policies such as those relating to travel and expense reimbursement, use of the telephone system and the Internet, or employee conduct generally, or where the data are needed for compliance or billing purposes. More frequent access to such data may occur incidental to an email surveillance program, if and to the extent permitted by applicable laws.

Where required by applicable law, when we ask you to provide personal data to us on a mandatory basis, we will inform you of this at the time of collection and in the event that particular information is required by the contract or statute this will be indicated. Failure to provide any mandatory information will mean that we cannot carry out certain HR processes. For example, if you do not provide us with your bank details, we will not be able to pay you. In some cases it may mean that we are unable to continue with your employment or

engagement as the Company will not have the personal data we believe to be necessary for the effective and efficient administration and management of our relationship with you.

Apart from personal data relating to you, you may also provide us with personal data of third parties, notably your dependents and other family members, for purposes of HR administration and management, including the administration of benefits and to contact your next-of-kin in an emergency. Before you provide such third-party personal data to us you must first inform (and where required by applicable law, obtain consent from) these third parties of any such data which you intend to provide to us and of the processing to be carried out by us, as detailed in this Data Privacy Notice.

3.0 WHAT ARE THE PURPOSES FOR WHICH DATA ARE PROCESSED?

Your personal data are collected and processed for business purposes, in accordance with applicable laws and any applicable collective bargaining agreements, and with your consent where required. The specific purposes for which we collect and process your data include:

A. recruitment and hiring (including, for example, deciding whether and when to make an offer of employment, conducting any pre-employment checks including those required by applicable law, and purposes relating to your location of employment);

B. to support HR administration and management and maintaining and processing general records necessary to manage the employment, worker or other relationship and operate the contract of employment or engagement, including:

    a. providing and administering compensation, benefits and incentive schemes and reimbursement of business costs and expenses and making appropriate tax and social security deductions and contributions;

    b. managing and operating appraisal, conduct, performance, capability, absence and grievance related reviews, allegations, complaints, investigations and processes and other informal and formal HR processes and making related management decisions;

    c. processing information about absence or medical information regarding physical or mental health or condition in order to: assess eligibility for incapacity or permanent disability related remuneration or benefits, determine fitness for work, facilitate a return to work; make adjustments or accommodations to duties or the workplace;

    d. make management decisions regarding employment or engagement or continued employment or engagement or redeployment;

    e. and conduct related management processes; and training, development, promotion, career and succession planning and business contingency planning;

C. allocating and managing duties and responsibilities and the business activities to which they relate, including business travel, and for planning, managing, and carrying out restructuring or redundancies or other change programs;

D. conducting surveys or other analyses for benchmarking and identifying improved ways of working, general business, operations, and office planning, and reasons related to employee relations and engagement at work;

E. operating email, IT, internet, social media, HR related and other company policies and procedures. To the extent permitted by applicable laws, OpenAI carries out monitoring of the Company's IT systems to protect and maintain the integrity of the Company's IT systems and infrastructure; to ensure

compliance with the Company's IT policies and to locate information through searches where needed for a legitimate business purpose;

F. complying with applicable laws and regulation (for example maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws and regulation to which OpenAI the Company is subject in the conduct of its business), and satisfying our regulatory obligations to supervise the persons employed or appointed by the Company to conduct business on its behalf, including preventing, detecting and investigating a wide range of activities and behaviors, whether relating to specific business dealings or to the workplace generally, and liaising with regulatory authorities;

G. to the extent permitted or required by applicable law, ensuring equality of opportunity and diversity with regard to personal characteristics protected under applicable anti-discrimination laws;

H. for business operational and reporting documentation such as the preparation of annual reports or tenders for work or client team records, and planning, due diligence and implementation in relation to a commercial transaction or service transfers involving OpenAI that may impact your relationship with the Company, (for example mergers and acquisitions or a transfer of your employment under applicable automatic transfer rules);

I. to operate the relationship with third-party customer and suppliers including the disclosure of relevant vetting information in accordance with relevant requirements of regulated customers, or disclosure of information to data processors for the provision of services to the Company;

J. where relevant for publishing appropriate internal or external communications or publicity material, including via social media in appropriate circumstances;

K. to comply with reference requests where the Company is named by the individual as a referee;

L. to enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you;

M. to comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment), whether within or outside your country.

In addition, personal data will be collected for other purposes permitted by applicable laws, with your consent (where required) and upon notice.

Sensitive personal data may be collected and processed by the Company for the following purposes, to the extent permitted or required by applicable law, and with your consent whenever required by applicable law:

A. documentation such as work permits, details of residency, proof of citizenship will be processed to assess and review eligibility to work for the Company in the jurisdiction in which you work;

B. financial information will be processed to ensure payment of wages, salaries, fees or other amounts owed to you, or benefits, as relevant to your situation;

C. information related to your racial or ethnic origin, religion, philosophical or political belief, sexual orientation or sexual life, or disability status may be used for the collection of statistical data, or where required to record such characteristics to comply with equality and diversity requirements of applicable local legislation, or to keep the Company's commitment to equal opportunity under review. It may be used in the event of a complaint under the Company's grievance, whistleblowing, anti-bullying and harassment or similar policies where such characteristics or information are relevant to the particular

complaint, in order to comply with employment law obligations;

D. health and medical information may be used to comply with employment, health and safety or social security laws, such as to provide statutory incapacity or maternity benefits, avoid breaching legal duties to you, to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to administer the Company's private medical and long term disability schemes, to make reasonable accommodations or adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard;

E. trade union membership may be recorded to ensure that you receive any relevant rights that you may have in connection with any trade union membership, as required to enable us to meet our obligations under employment law; and

F. biometric data for purposes of building access and security.

4.0 Disclosures of personal data

Within OpenAI, your personal data can be internally accessed or disclosed on a confidential basis to:

- local and global Human Resources staff, including managers and team members;
- local, regional and executive management responsible for managing or making decisions in connection with your relationship with the Company or when involved in an HR process concerning your relationship with the Company (including, without limitation, staff from Compliance, Legal, Employee Relations and Information Security);
- system administrators; and
- where necessary for the performance of specific tasks or system maintenance by staff in OpenAI teams such as the Finance and IT Department and the Global HR information systems support team.

In addition, we may share personal data with the following:

Other OpenAI employees	Certain basic personal data, such as your name, location, job title, contact information, employee number and any published skills and experience profile may also be accessible to OpenAI employees.
Third parties with whom we work	Examples of third parties with whom your data will be shared include tax authorities, regulatory authorities, OpenAI's insurers, bankers, IT administrators, lawyers, auditors, investors, consultants and other professional advisors, third-party partners and potential third-party partners (for instance, third parties with whom OpenAI is exploring a strategic partnership), and administrators of the Company's benefits programs. The Company expects such third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security. We may also disclose personal data to third parties that provide us with services, such as hosting, supporting and maintaining the framework of our HR information systems, or providing services on our behalf (payroll provider) In these cases, these third parties act as a "data processor" to carry out tasks upon our instructions for the above mentioned purposes. In this case your personal data will only be disclosed to these parties to the extent necessary to provide the required services.

Business transfers	If we are involved in strategic transactions, reorganization, bankruptcy, receivership, or transition of service to another provider (collectively, a "Transaction"), your personal iInformation and other information may be disclosed in the diligence process with counterparties and others assisting with the Transaction and transferred to a successor or affiliate as part of that Transaction along with other assets.
Certain interconnecting systems such as local payroll and benefits systems.	Data contained in such systems may be accessible by providers of those systems, their associated companies and sub-contractors.
National or other government authorities	In order to comply with a legal obligation to which we are subject, or to establish, exercise or defend legal rights. This is for example the case in the framework of imminent or pending legal proceedings or a statutory audit.

Disclosures and sharing are made on the basis of your consent, where required by applicable laws.

5.0 Security of data

OpenAI has implemented appropriate technical, physical and organizational measures aimed at providing a level of security appropriate to the risk.

If you are in possession of personal data of any kind (e.g., data collected in emails, address books, Excel spreadsheets or contained in curricula vitae or elsewhere) you must ensure that the data are kept in a safe place where unauthorized access cannot occur. Where data is retained in hard copy, storage in a locked drawer or cabinet, accessible only to authorized individuals, is generally the most effective means of securing the data. Where data is kept in electronic form, appropriate password protection and appropriately secured areas should be used. You must comply with the security obligations contained in the Company's applicable policies.

You should not create, copy or export personal data relating to any other person outside of official company storage locations and systems except where necessary for a specific authorized and lawful purpose under this Data Privacy Notice. In this event appropriate measures must be taken to protect the confidentiality and integrity of the data during the processing. Once the relevant processing is complete, steps should be taken to store or return the relevant data within the official storage locations/systems with all less formally held records (e.g. local folders, hard copies, emails saved outside of formal managed folders) securely erased.

6.0 Retention of personal data

Subject to applicable law, the Company endeavors to ensure that personal data are kept as current as possible and that irrelevant or excessive data are deleted or made anonymous as soon as reasonably practicable.

The Company's general approach is to only retain personal data for as long as is required to satisfy the purpose for which it was collected by us or provided by you. This will usually be the period of your employment/contract with us, plus the length of any applicable statutory limitation period, or mandatory retention period (e.g., for tax or pensions information), following your departure. If you are an applicant and are unsuccessful in your application, the Company may retain your personal data to periodically notify you of new job openings, where required under applicable law, on the basis of your voluntary consent. If you do not want us to retain your personal data for these purposes, you can let us know by responding to our email notifications or contacting us at hr@OpenAI.com.

7.0 NOTICE OF CHANGES

The Company may change or update this Data Privacy Notice at any time, and we will inform you that we have updated the Data Privacy Notice in accordance with applicable law.

COUNTRY/JURISDICTION SPECIFIC ADDENDUMS

European Economic Area, UK and Switzerland Addendum
US and Canada Addendum
Japan Addendum
Korea Addendum
Singapore Addendum
Australia Addendum
India Addendum
United Arab Emirates (ADGM) Addendum
Brazil Addendum

9

EUROPEAN ECONOMIC AREA, UNITED KINGDOM AND SWITZERLAND DATA PRIVACY/FAIR PROCESSING NOTICE

Data Controller

The OpenAI entity to which you submit an application for employment or with which you have your contract (the "Company"), along with OpenAI OpCo, LLC and OpenAI Ireland Limited, act as joint controllers of your personal data - which means OpenAI and those two affiliates jointly determine how to use your personal data in connection with your application and employment - but only as described in this Policy. The Company will be primarily responsible for providing you with any information to which you are entitled, and responding to your requests, under data protection law.

Contacts

You may contact the Company's Data Protection Officer ("DPO") at any time if you have any concerns about the processing of your personal data or any data protection issue. The DPO can be reached at hrprivacy@openai.com (please put in your subject line, "Attention: DPO").

If you have any questions regarding the processing of your personal data or if you believe your privacy rights have been violated, please contact your local Human Resources contact hr@openai.com or, where applicable, the DPO. If you are aware of an unauthorised disclosure of data, please report this immediately to hrprivacy@openai.com.

LEGAL BASES FOR PROCESSING

Personal data

Whenever the Company processes your personal data, we do so on the basis of a lawful condition ("legal basis") for processing. Processing of special categories of data is always justified on the basis of an additional condition.

In the majority of cases, the processing of your personal data will be justified on one of the following bases:

- the processing is **necessary for compliance with a legal obligation** to which the Company is subject (for example, disclosing the information to tax authorities, making statutory payments, avoiding unlawful termination, avoiding unlawful discrimination, meeting statutory record keeping requirements or health and safety obligations);
- where there is no legal obligation, we will process your data where the processing is **necessary for the performance of a contract** to which you are a party or in order to take steps at your request prior to entering into such a contract (for example collecting bank details to pay your salary or processing information to provide you with the contractual benefits you are entitled to); or
- where the above two grounds do not apply, we may process your personal data where the processing is necessary for the **legitimate interests pursued by the Company** (being those purposes described in the section 3.0 of the main policy), except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data (for example reviewing your performance at work).

- For staff in Germany only: if you are considered an “employee” as defined in the German Federal Data Protection Act (Bundesdatenschutzgesetz)[1], and if we investigate criminal offenses, we rely on the special German legal basis for such investigations, but only if there is a documented reason for the suspicion that an employee committed a criminal offence in the employment relationship.

We will on occasion process your personal data for the purpose of legitimate interests pursued by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data.

In exceptional circumstances where we have no legitimate interest in processing but you ask us to process data for a particular purpose we will occasionally carry out the processing on the basis of your consent (for example if you ask us to provide pay information to a bank for a mortgage application made by you). Where we rely on your consent, we will make this clear at the relevant time to you.

In some circumstances, data will sometimes be collected indirectly from monitoring devices or by other means (for example, building and location access control and monitoring systems, CCTV, telephone logs and recordings, instant message logs and email and Internet access logs), if and to the extent permitted by applicable laws. In these circumstances, the data may be collected by OpenAI or a third party provider of the relevant service. This type of data is generally not accessed on a routine basis but access is possible. Access can occur, for instance, in situations where OpenAI is investigating possible violations of Company policies such as those relating to travel and expense reimbursement, use of the telephone system and the Internet, or employee conduct generally, or where the data are needed for compliance or billing purposes or to ensure the safety of our staff and protection of property. More frequent access to such data may occur incidental to an email surveillance program, if and to the extent permitted by applicable laws.

Special categories of data

The special categories of personal data that may be processed by the Company are set out in this Data Privacy Notice. Where we process special categories of data it will be justified by a legal basis set out above and also by one of the following additional conditions:

- the processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws;
- the processing is necessary for preventative or occupational medicine, for the assessment of your working capacity, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services, to the extent permitted by applicable laws;
- the processing is necessary to protect your vital interests or of another person where you are physically or legally incapable of giving consent (for example in exceptional emergency situations, such as a medical emergency);
- the processing is necessary for purposes authorised by applicable law.
- the processing is necessary for the establishment, exercise or defence of legal claims; or
- in exceptional circumstances the processing is carried out subject to your explicit consent (as explained below).

We will occasionally seek your consent to certain processing which is not otherwise justified under one of the above conditions. If consent is required for the processing in question, it will be sought from you separately to ensure that it is freely given, informed and explicit. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any

[1] Employees (as defined by sec. 26 (8) of the German Federal Data Protection Act) are in particular: dependently employed workers, including temporary workers contracted to the borrowing employer; persons employed for occupational training purposes; persons undergoing rehabilitation.

such consent. You should be aware that it is not a condition or requirement of your employment to agree to any request for consent from the Company.

Personal data relating to criminal convictions and offences will only be processed where authorised by applicable laws. For example, an allegation of a criminal offence or conviction arising during your relationship with the Company may be processed where required or authorised by applicable law where we have a legal or regulatory requirement to report an offence; or where applicable laws authorise the Company to process information about the offence (e.g. in a disciplinary process) for the purpose of making decisions regarding your relationship with the Company.

INTERNATIONAL TRANSFER OF PERSONAL DATA

From time to time your personal data (including special categories of personal data) will be transferred to OpenAI entities to process for the purposes described in this Data Privacy Notice. This will be applicable for example where the relevant entity or a manager from that entity is responsible for conducting or approving the relevant process or the data is part of a global directory where other individuals need to have access.

These entities or managers are located within the European Economic Area (EEA), United Kingdom, Switzerland and elsewhere in the world (for example, OpenAI OpCo, LLC based in the United States).

Personal data may also be transferred to third parties (e.g. service providers or regulators as set out above), who may have systems or suppliers located outside the EEA, the United Kingdom or Switzerland. As a result, in some circumstances your personal data will be transferred to countries outside of the country in which you work or outside of the EEA, United Kingdom or Switzerland to countries whose data protection laws may be less stringent than yours.

Therefore, we may transfer your personal data to countries within the EEA, to the United Kingdom or Switzerland and to countries outside of the EEA, the United Kingdom or Switzerland, provided that

a) such countries provide for an adequate level of data protection according to the assessment of the competent authority ("Adequacy Decision", e.g. pursuant Art. 45 (UK) GDPR[2]),

b) the Company will ensure that appropriate or suitable safeguards are in place to protect your personal information and that transfer of your personal information is in compliance with applicable data protection laws, or

c) we may rely on a statutory exception (e.g., Art. 49 (UK) GDPR).

The countries to which data may be transferred are: the United States.

When transferring personal data to recipients in the US we may rely on the EU-U.S. Data Privacy Framework (EEA) or its respective UK Extension or the Swiss-U.S. Data Privacy Framework ("**DPF**"), which ensures an adequate level of protection for recipients certified under the DPF.

Where required by applicable data protection laws, in particular because there is no Adequacy Decision, the Company has ensured that service providers (including other OpenAI group entities) sign standard contractual clauses or similar transfer mechanisms as approved by the European Commission (Art. 46 GDPR), UK government (Art. 46 UK GDPR) or other supervisory authority with jurisdiction over the relevant Company exporter. You can obtain a copy of any standard contractual clauses in place and the implemented appropriate safeguards which relate to transfers of your personal data by contacting hrprivacy@openai.com. Please note that such copy may be redacted to the extent necessary to protect business secrets or other confidential information.

[2] A list of the European Commission's adequacy decisions can be found here.

OpenAI has an intra-group data transfer agreement in place which regulates cross-border transfers of your data within the OpenAI group.

Retention of personal data

Germany: We will usually keep your personal data throughout the time that you work for us and for three years after you leave after which it will be destroyed unless there is a good reason to keep it (or any part of it) for longer (for example, for the purposes of compliance with our obligations relating to audits or tax). Once you are no longer a staff member we will retain and then securely destroy your personal data in accordance with applicable law or any data retention policy available in place from time to time. If you are an applicant and are unsuccessful in your application, we generally keep your personal data for the duration of the application process and for four months after we have informed you that your application was not successful, unless you have given us your consent to retain your application for a longer period of time. Where relevant, we may retain your application/personal data for a longer time for the exercise of, or defense against, legal claims. **Switzerland**: If you are an applicant and are unsuccessful in your application, we generally keep your personal data for the duration of the application process and for three months thereafter, unless you ask or allow us to retain your application for a longer period of time. Where relevant, we may retain your application/personal data for a longer time for the assessment or exercise of, or defense against, legal claims.

Your rights as a data subject

Subject to the conditions and limitations set forth in GDPR, you have the following rights in respect of your personal data.

Right	Description
Right to access, correct and delete your personal data	The Company aims to ensure that all personal data are correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to the Company so that we can ensure that your data is up-to-date. You have the right to request access to any of your personal data that the Company may hold, and to request correction of any inaccurate data relating to you. You furthermore have the right to request deletion of any irrelevant data we hold about you. If you are an employee, you can see and update some of this data yourself via your applicable HR system account. However, to correct / update certain information, you will need to contact hr@openai.com.
Data portability	Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to the Company in a structured, commonly used and machine-readable format, and also to require us to transmit it to another controller where this is technically feasible.

Right to restriction of processing	You have the right to restrict our processing of your personal data where: ● you contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy; ● where the processing is unlawful but you do not want us to erase the data; ● where we no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims; or ● where you have objected to processing justified on legitimate interest grounds (see below) pending verification as to whether the Company has compelling legitimate grounds to continue processing. Where personal data is subjected to restriction in this way, we will only process it with your consent or for the establishment, exercise or defence of legal claims.
Right to withdraw consent	Where we have relied on your consent to process particular information and you have provided us with your consent to process data, you have the right to withdraw such consent at any time. You can do this by: ● in some cases, deleting the relevant data from the relevant HR system (although note that in this case it may remain in back-ups and linked systems until it is deleted in accordance with our data retention policy); or ● contacting your local Human Resources contact. It will only however be rarely that we rely on your consent to process personal data for your employment or engagement.
Right to object to processing justified on legitimate interest grounds	Where we are relying upon legitimate interest to process data, then you have the right to object to that processing. If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims. Where we rely upon legitimate interest as a basis for processing, we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.
Right to complain	You also have the right to lodge a complaint with a supervisory authority if you consider that the processing of your personal data infringes applicable law. For a list of supervisory authorities in the EU/EEA please see here, for the UK here and for Switzerland here. You have the right to lodge such a complaint at any time, however, we would encourage you to contact us in the first instance to allow us to remedy any complaints.
Right to control your digital legacy (France only)	You have the right to issue directives concerning the disposition of your personal data after your death, in the conditions set forth in Art. 85 of the January 6, 1978 Law on Computing Technologies and Freedoms.

U.S. / CANADA

OpenAI U.S. and Canada Privacy Policy for Employees, Applicants, Contractors, and Guests

Last Updated: October 1, 2024

OpenAI, D.B.A. Summerlight Technologies Ltd ("OpenAI", "we", "us", or "our") respects your privacy and is committed to protecting your personal information.

This Privacy Policy ("Policy") outlines how we collect and use personal information about you leading up to, during, and after your employment, contractual engagement, or other relationship you may have with us. This Policy applies to current and former employees, job applicants, current or former independent contractors, and guests ("you").

This Policy describes the categories of personal information that we collect, how we use your personal information, how we secure your personal information, and when we may share your personal information with third parties. This Policy also describes your rights regarding the personal information that we hold about you and how you can access your personal information. We will only use your personal information in accordance with this Policy, unless otherwise required by applicable law. To the extent this Policy conflicts with applicable law in your jurisdiction, applicable law will control.

This Policy does not cover your use of OpenAI products as a user or customer, or outside of your employment, working relationship, or other assignment with OpenAI. To learn more about OpenAI's data collection practices that cover your use of OpenAI 's website, products, and services, please read our Privacy Policy, available at https://OpenAI.com/privacy.

This Policy is not intended and shall not be read to create any express or implied promise or contract for employment, for any benefit, or for specific treatment in specific situations. Canadian employees should review the section below "*Additional Information for Canadian Residents*" that is specific to Canadian residents. Nothing in this notice should be construed to interfere with OpenAI's ability to process your data for purposes of complying with our legal obligations, or for investigating alleged misconduct or violations of company policy or law, subject to compliance with local legal requirements.

Collection of Personal Information

In this Policy "Personal Information" means information that directly identifies an individual (such as a name) or that is associated with an identified individual (such as a home address in combination with a name), or information that can be used to identify a specific individual (such as a mobile phone number or home address), or as the term may otherwise be defined in applicable law.

We collect, use, and store (collectively "process") different types of Personal Information about you in the operation of our business. For example, if you are an employee, we process Personal Information about you primarily for managing our employment relationship with you and managing your interactions with workplace facilities/information systems. If you are a former employee, we process Personal Information about you primarily for legal compliance. If you are an independent contractor, we process your Personal Information to manage your engagement with OpenAI and access to our facilities and information systems. If you are a candidate, we process your Personal Information to engage with you about OpenAI career opportunities and consider your application for employment.

The Personal Information we process includes the following:

Categories of Personal Information	Examples of Personal Information	Categories of Collection Sources
Identifiers	First and last name, mailing address, employee or contractor ID, photo, signature, telephone number, email address, tax information, payroll information, withholdings, and other similar identifiers.	You, service providers, public sources.
Professional or employment-related information	Current or past job history or performance evaluations, resume, cover letter, job title, wage and benefit information, compensation, disciplinary or employment records, job restrictions, payroll information, and workplace illness and injury information.	You, your references, other employees, service providers, public sources.
Education information	Educational history, academic degrees, professional qualifications, certifications, and skills.	You, service providers, public sources.
Internet or other electronic network activity	Application data, such as emails sent and received from your work email address, OpenAI systems and software usage data, OpenAI device information and activity; and cookies when you interact with our recruiting website as described more fully in our Privacy Policy at www.OpenAI .com/privacy.	You, service providers, your devices.
Sensitive Personal Information	Social Security number or social insurance number driver's license number, passport number, state identification number, racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, medical information, financial account information, and health insurance information.	You.

Protected classification characteristics	Age (40 years or older), race, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, and veteran or military status. If you are employed in Canada, these characteristics may differ by province and are any characteristic protected by applicable provincial human rights legislation. This may include but is not limited to: indigenous identity, race, colour, ancestry, place of origin, political belief, religion, marital status, family status, physical or mental disability, sex, sexual orientation, gender identity or expression, or age of that person or because that person has been convicted of a criminal or summary conviction offence that is unrelated to the employment.	You.
Biometric information	Fingerprint and handprint scans for employee- only for the purpose of providing access to OpenAI offices in certain locations.	You.
Geolocation data	Physical location or building access data.	You, service providers.

Electronic, visual, and audio information	Video conference or call recordings or video surveillance for security purposes	You, service providers.
Inferences drawn from other Personal Information	Summary about an employee's abilities, job performance, or preferences.	You.

The categories above include categories of Personal Information we have collected in the preceding 12 months. It is important that the Personal Information we hold about you is accurate and current. Please keep us informed if your information changes during your employment by emailing hr@openai.com.

How We Collect Personal Information
We will collect information from the following sources:

Directly from you. For example, if you visit our office, respond to our employment offer, submit information via our websites or applications, complete forms or surveys that we provide to you, exercise your employment rights, provide documents, or otherwise voluntarily provide Personal Information to us.

From other employees or third parties. For example, when collecting feedback from colleagues as part of regular employee reviews or information on your past employment performance or conduct from your references or recruiters.

From our service providers. For example, we hire vendors to conduct background checks in accordance with applicable law. We also use staffing agencies to manage our contingent workforce who may collect Personal Information from personnel on our behalf.

From your activities at work based on, for example, office building entry, OpenAI systems and software usage, your work computer, and Internet logs.

We may also collect publicly available information about you from third parties.

How We Use Your Personal Information

We use Personal Information as needed in performance of our employment or other relationship with you or to comply with our legal obligations, including for the following legitimate business purposes:

- Managing our recruitment process and our employment relationship with you including:
    - evaluating an applicant's qualifications and suitability for employment;
    - administering pre- and post-employment tests and training activity;
    - conducting criminal and other background checks;
    - completing the employment onboarding process;
    - timekeeping, payroll, direct deposit authorization, and expense report administration;
    - administration of benefits, leaves of absence, and maintaining emergency contact information;
    - employee training and development;
    - workers' compensation claims management;
    - performing workforce analytics, data analytics and benchmarking; or
    - other human resource purposes.
- Preparing and maintaining legally required records, such as I-9 forms, EEO-1 forms, and affirmative action plans, or, if you are employed in Canada, T4s or other tax or regulatory reporting forms.
- Conducting accounting activities, workplace investigations, and internal audits.
- Meeting tax obligations, complying with applicable law, and complying with health and safety obligations.
- Maintaining commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Managing and monitoring employee access to company facilities, equipment, and systems.
- Preventing and detecting unlawful and inappropriate use of company credit cards, systems and assets and countering loss of company data.
- Investigating and enforcing compliance with company policies and procedures.
- Detecting and preventing unlawful and inappropriate use of company resources and countering loss of company data.
- Detecting, protecting against, responding to, and security incidents, malicious, deceptive, fraudulent, or illegal activity; and then prosecuting those responsible for that activity.
- Exercising or defending the legal rights of the Company, its employees or affiliates.
- Conducting business management and planning including internal administration with our affiliated entities.
- Engaging in corporate transactions, such as evaluating potential mergers and acquisitions, which require review of employee records.

Data Sharing

We may share your Personal Information with our trusted affiliates, contractors, and vendors (collectively, “service providers”) who provide services to us or on our behalf, or otherwise support our relationship with you. These service providers include, but are not limited to, payroll processors and benefits or leave administration providers.

As part of protecting your Personal Information, we require all our service providers to implement appropriate security measures consistent with our policies and data security obligations. We do not permit our providers to use your Personal Information for purposes unrelated to the terms of their engagement with us. As such, we only permit them to use your Personal Information for those purposes specified in accordance with our instructions.

We may also share your Personal Information for the following additional purposes where permitted or required by applicable law:

- Complying with court orders, subpoenas, lawful discovery requests and as otherwise permitted or required by law or regulation. We may be required by law at times, to provide certain information to government or law enforcement agencies, or to parties to civil lawsuits.
- Detecting and preventing fraud or other illegal or unauthorized activities.
- During emergency situations or where necessary to protect the safety of persons.
- Where the Personal Information is publicly available.
- If a business transfer or change in ownership occurs.
- For additional purposes with your consent where such consent is required by law.

Data Storage, Retention and Disposal

The information we collect may be processed and stored in the United States or in other countries where we or our affiliates or service providers process our data. We take steps to ensure that data is processed according to this Policy and to ensure Personal Information is adequately protected in accordance with applicable law. Your personal information may be subject to access by local government authorities in accordance with applicable law.

Except as otherwise permitted or required by applicable law or regulation, we will only retain your information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any operational, legal, accounting, or reporting requirements. Under some circumstances we may anonymize your information so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your express consent. Once you are no longer an employee or contractor of OpenAI we will retain or destroy your Personal Information in accordance with our records retention policy and applicable laws and regulations.

If you are an applicant and are unsuccessful in your application, the Company may retain your personal data to periodically notify you of new job openings. If you do not want us to retain your personal data for these purposes, you can let us know by responding to our email notifications or contacting us at hr@openai.com.

Additional Information for California Residents

This section supplements the above Policy and applies solely to California residents. We have issued this notice to comply with the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act (CPRA) and implementing regulations.

This section does not address or apply to our information practices that are not subject to the CCPA, including publicly available, deidentified, or aggregate information, or information covered by the Health Insurance Portability and Accountability Act, California Confidentiality of Medical Information Act, or the Fair Credit Reporting Act.

How we Share Your Personal Information

We do not sell your Personal Information and do not share your Personal Information for targeted advertising purposes. We have not sold or shared your Personal Information for targeted advertising purposes in the preceding 12 months. We do not have actual knowledge that we sell or share the Personal Information of individuals under 16 years of age. We do not share your sensitive Personal Information for purposes other than for the purposes of managing and facilitating your employment or contract relationship with us or as otherwise authorized by you.

Your California Rights

The CCPA provides California residents with specific rights regarding their Personal Information.

- **Right to Know**: You may have the right to request information about the Personal Information we have collected about you, the purpose of our collection, and the source of the data. You may also have the right to know the categories of third parties to whom we have disclosed your Personal Information, for what purpose, and what Personal Information has been disclosed.

- **Right to Access**: You may have the right to request information about how we process your Personal Information and to obtain a copy of that Personal Information.

- **Right to Portability**: You may obtain a copy of your Personal Information in a structured, commonly used, and machine-readable format and to have that information transmitted to another organization in certain circumstances.

- **Right to Correction**: You may have the right to request that we modify or correct errors in the Personal Information that we have collected from you. However, please note that we may not accommodate a request to change Personal Information if we believe that doing so would violate any law, legal requirement or rights of another person, or cause the information to be incorrect.

- **Right to Deletion**: You may have the right to request the deletion of your Personal Information that we have collected from you.

- **Right to Limit Use and Disclosure.** Subject to certain conditions and exceptions, you may have the right to limit the use and disclosure of sensitive Personal Information. However, we do not engage in activities triggering this right.

Note, this section only applies to rights and practices pursuant to the CCPA. These rights are in addition to any rights that may be available to you under the California Labor Code. To the extent you wish to exercise any rights pursuant to the Labor Code, please contact hr@openai.com.

1. Rights around Automated Decision-Making Technology

We do not use your personal information for automated decision-making. If OpenAI were to use automated decision-making technology, it may be used to infer information about your work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, and movement. If OpenAI were to use automated decision-making, you would have the right to request information about such automated decision- making technology and processing, and its results. You would also have the right to opt-out of decision-making technology and profiling and the right to opt-out of cross-context behavioral advertising.

2. How to Exercise Your Rights

If you have any questions regarding the information contained in this Policy or would like to exercise your California rights, please contact us using either method below:

Send an email to: hr@openai.com

Call us at: 1 (844) 534-9165

You can also reach out to our Data Protection / Privacy Officer at hrprivacy@openai.com (please put in the subject line, “Attention: DPO”).

When submitting a request, we may require additional information from you or take other steps to verify your identity and your right to access the Personal Information we hold about you. This is done to protect your privacy and maintain security. We may charge you a reasonable fee in instances that require a disproportionate effort, but we will advise you of any fee in advance. We may decline to process requests that are frivolous or unreasonably repetitive or burdensome, risk the privacy or impact the rights of others, or are extremely impractical. An authorized agent may also submit a request on your behalf.

3. Non-Discrimination

California law ensures that you are free from discrimination or retaliation when you exercise your California privacy rights, and we will not discriminate or retaliate against you for exercising any rights.

Additional Information for Canadian Residents

This information supplements the above policy and applies to Canadian residents. In general, the employer is permitted under Canadian law to collect, use and disclose personal information about employees without consent but with notice where reasonable to establish, manage or terminate the employment relationship. We process the personal information of applicants and employees in accordance with this notice. In circumstances where consent may be required by applicable law, we will seek your consent.

If you are a contractor or guest, by sharing your personal information with us you consent to the processing of that personal information in accordance with this policy.

We will retain your personal information for the period required as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. If we use your personal information to make a decision that affects you, we will retain it for at least one year so you may exercise your right to access it.

4. Rights under Canadian Law

- **Right to Access**: you may have the right to request information about how we process your Personal Information and to obtain a copy of that Personal Information.

- **Right to Correction**: you may have the right to request that we correct errors in the Personal Information that we have collected from you.

An individual's right to access or seek correction of their personal information is not absolute but is subject to limitations permitted or required by applicable law.

5. Questions, Complaints and Requests for Access or Correction

Questions regarding the information contained in this Policy, requests to access or correct your personal information or complaints can be directed to:

Send an email to: hr@openai.com

Call us at: 1 (844) 534-9165

You can also reach out to our Privacy Officer at hrprivacy@openai.com (please put in the subject line, "Attention: DPO").

When submitting a request, we may require additional information from you or take other steps to verify your identity Personal Information we hold about you. This is done to protect your privacy and maintain security. We will respond to any requests in accordance with applicable law.

OpenAI Korea, Ltd.

Personal Information Protection Policy (Employee)

1. General Provisions

OpenAI Korea, Ltd. (the "**Company**") endeavors to protect the personal information of its employees ("**Employees**") and comply with all applicable privacy laws and regulations, including the Personal Information Protection Act (the "**PIPA**"). The Company's personal information protection policy for Employees' personal information (this "**Privacy Policy**") can be amended in accordance with applicable laws and regulations, regulatory instructions and the Company's internal policies.

2. Purposes of Processing Personal Information and Items of Personal Information to be Processed

Pursuant to Article 15(1)1 of the PIPA, the Company will collect and use some or all of Employees' personal information listed below with their consent for the following purposes, in relation to the employment relationships with them.

General Personal Information

Mandatory		
Items of Personal Information to be Processed	**Personal details**	Name(s), gender, nationality(ies), civil / marital status, date of birth, age, contact details, immigration / eligibility to work information, driver's license, unique identification numbers, languages spoken, next-of-kin / dependent / emergency contact information, reasonable adjustments information;
	Information about your **recruitment and hire**	Skills and experience, qualifications, references, CV and application, information collected during the recruitment and interview process, results of credit reference check, financial sanction check, right to work verification, outcome of your application, details of any offer made;
	Information about your **employment and engagement**	Contract/terms of employment or engagement, work contact, employee or payroll number, photograph, work location default hours, default language, time zone and currency for location, worker ID and system IDs, work biography, assigned business unit or group, reporting line, employment type (e.g., contingent worker/employee, full/part time), your hire/contract begin and end dates, cost center, working hours and patterns, reason(s) for a change in work status, exit interviews, references provided, and status (active/inactive/terminated). If you are subject to a redundancy or restructuring, we may collect information related to this including change plans, organization charts, consultation records, and selection and redeployment data;
	Regulatory data	Records of registration with any applicable regulatory authority, regulated status, regulatory certificates and references;

	Information related to your **compensation and benefits**	Remuneration information, payments for leave/absence, bank account details, grade, tax information, benefit recipient information, details of available benefits, benefit coverage start and end date, expense claims and payments, loans, deductions, salary sacrifice arrangements, childcare vouchers, and share scheme information;
	Information about a **leave or absence**	If you go on leave (such as family leave, or other types of leave such as bereavement leave, jury service, or compassionate leave) or otherwise take a term of absence while at OpenAI, we may collect information such as attendance and absence records (including dates and types of absence and relevant approvals). To the extent required by law, we may also collect other information about a specific type of leave of absence, including fit notes details of incapacity, work impact and adjustments, treatment and prognosis, manager and HR communications, return to work interviews, meeting records, medical reports, occupational health reports;
	Information about **flexible working procedure**	Requests, consideration, correspondence, meeting notes and outcome records;
	Information related to your **job performance**	Feedback, appraisals, and performance management and review information, outcomes and objectives, talent program assessments and records, succession plans;
	Information about your **training and development**	Training and development needs, training received, and assessments completed;
	Information about **disciplinary actions and grievances**	Allegations, complaints, investigations, and proceeding records and outcomes;
	Health and safety data (as applicable)	Health and safety audits, screening requests and results, risk assessments, incident reports;
	Information related to your **use of our offices, company devices, and other company assets**	Data generated from monitoring and management of company assets (e.g., closed circuit television footage, system and building login and access records including badge swipes, keystroke, download and print records, information about calls or meetings, data caught by IT security programs and filters);
	Information about **employee claims, complaints and disclosures**	Subject matter of litigation and complaints, pre-claim conciliation, communications, settlement discussions, claim proceeding records, incident reporting and disclosures. This also may include personal data related to OpenAI's (or a third parties') establishment, exercise and/or defense of rights generally; personal data required to comply with applicable law, or personal data relating to responses to law enforcement or government requests;
	Biometric information	Biometric information such as fingerprint and handprint only for the purpose of providing access to OpenAI offices in certain locations

	Other	Any other personal data you choose to disclose verbally or in writing to Company personnel during the course of recruitment or your engagement; informal opinion data generated in the course of recruitment or your engagement relating to the administration or management of the Company's relationship with you. This may include, for instance, information relating to the conduct of OpenAI's business, including carrying out roles and responsibilities, communications with colleagues and business partners, and internal reporting. Certain additional information will sometimes be collected where this is necessary and permitted by local applicable laws.
Purposes of Processing Personal Information	A. recruitment and hiring (including, for example, deciding whether and when to make an offer of employment, conducting any pre-employment checks including those required by applicable law, and purposes relating to your location of employment); B. to support HR administration and management and maintaining and processing general records necessary to manage the employment, worker or other relationship and operate the contract of employment or engagement, including: a. providing and administering compensation, benefits and incentive schemes and reimbursement of business costs and expenses and making appropriate tax and social security deductions and contributions; b. managing and operating appraisal, conduct, performance, capability, absence and grievance related reviews, allegations, complaints, investigations and processes and other informal and formal HR processes and making related management decisions; c. processing information about absence or medical information regarding physical or mental health or condition in order to: assess eligibility for incapacity or permanent disability related remuneration or benefits, determine fitness for work, facilitate a return to work; make adjustments or accommodations to duties or the workplace; d. make management decisions regarding employment or engagement or continued employment or engagement or redeployment; and e. conduct related management processes; and training, development, promotion, career and succession planning and business contingency planning; C. allocating and managing duties and responsibilities and the business activities to which they relate, including business travel, and for planning, managing, and carrying out restructuring or redundancies or other change programs; D. conducting surveys or other analyses for benchmarking and identifying improved ways of working, general business, operations, and office planning, and reasons related to employee relations and engagement at work;	

E. operating email, IT, internet, social media, HR related and other company policies and procedures. To the extent permitted by applicable laws, OpenAI carries out monitoring of the Company's IT systems to protect and maintain the integrity of the Company's IT systems and infrastructure; to ensure compliance with the Company's IT policies and to locate information through searches where needed for a legitimate business purpose;

F. complying with applicable laws and regulation (for example maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws and regulation to which OpenAI the Company is subject in the conduct of its business), and satisfying our regulatory obligations to supervise the persons employed or appointed by the Company to conduct business on its behalf, including preventing, detecting and investigating a wide range of activities and behaviors, whether relating to specific business dealings or to the workplace generally, and liaising with regulatory authorities;

G. for business operational and reporting documentation such as the preparation of annual reports or tenders for work or client team records, and planning, due diligence and implementation in relation to a commercial transaction or service transfers involving OpenAI that may impact your relationship with the Company, (for example mergers and acquisitions or a transfer of your employment under applicable automatic transfer rules);

H. to operate the relationship with third-party customer and suppliers including the disclosure of relevant vetting information in accordance with relevant requirements of regulated customers, or disclosure of information to data processors for the provision of services to the Company;

I. where relevant for publishing appropriate internal or external communications or publicity material, including via social media in appropriate circumstances;

J. to comply with reference requests where the Company is named by the individual as a referee;

K. to enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you;

L. to comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment), whether within or outside your country.

In addition, personal data will be collected for other purposes permitted by applicable laws, with your consent (where required) and upon notice; and

M. for purposes of building access and security

Optional

Items of Personal Information to be Processed	**Equality and diversity data** — Where permitted by law and provided voluntarily, data regarding gender, age, nationality, for example, to comply with regulations where applicable);
Purposes of Processing Personal Information	A. to the extent permitted or required by applicable law, ensuring equality of opportunity and diversity with regard to personal characteristics protected under applicable anti-discrimination laws;

Unique Identification Information

	Purposes of Processing Personal Information	Items of Personal Information to be Processed
Optional	◦ Performance of legal and administrative obligations imposed on the Company by the applicable laws and regulations	◦ Alien registration number (foreign employees only)

Sensitive Information

	Purposes of Processing Personal Information	Items of Personal Information to be Processed
Mandatory	A. Processing information about absence or medical information regarding physical or mental health or condition in order to: assess eligibility for incapacity or permanent disability related remuneration or benefits, determine fitness for work, facilitate a return to work; make adjustments or accommodations to duties or the workplace B. Complying with applicable laws and regulation (for example maternity or parental leave legislation, working time and health and safety legislation C. To the extent permitted or required by applicable law, ensuring equality of opportunity and diversity with regard to personal characteristics protected under applicable anti-discrimination laws D. Documentation such as work permits, details of residency, proof of citizenship will be processed to assess and review eligibility to work for the Company in the jurisdiction in which you work;	◦ Disability / reasonable adjustments information ◦ Fit notes details of incapacity, work impact and adjustments, treatment and prognosis, manager and HR communications, return to work interviews, meeting records, medical reports, occupational health reports ◦ Health and safety audits, screening requests and results, risk assessments, incident reports ◦ Race, nationality, religious belief and/or sexuality (which we treat as need-to-know and use, for example, to comply with federal contractor regulations where applicable) ◦ Biometric information such as fingerprint and handprint only for the purpose of providing access to OpenAI offices in certain locations ◦ Results of medical checkup, etc. ◦ Racial or ethnic origin; political opinions; religious or philosophical beliefs; physical or mental health (including details of accommodations or adjustments); trade union membership; sex life or sexual orientation; biometric and genetic data; or as otherwise

	E. Information related to your racial or ethnic origin, religion, philosophical or political belief, sexual orientation or sexual life, or disability status may be used for the collection of statistical data, or where required to record such characteristics to comply with equality and diversity requirements of applicable local legislation, or to keep the Company's commitment to equal opportunity under review. It may be used in the event of a complaint under the Company's grievance, whistleblowing, anti-bullying and harassment or similar policies where such characteristics or information are relevant to the particular complaint, in order to comply with employment law obligations; F. Health and medical information may be used to comply with employment, health and safety or social security laws, such as to provide statutory incapacity or maternity benefits, avoid breaching legal duties to you, to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to administer the Company's private medical and long term disability schemes, to make reasonable accommodations or adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard; G. Trade union membership may be recorded to ensure that you receive any relevant rights that you may have in connection with any trade union membership, as required to enable us to meet our obligations under employment law; and H. Biometric data for purposes of building access and security. I. Medical checkup and provision of medical supports J. Performance of legal and administrative obligations imposed on the Company by the applicable laws and regulations	defined by applicable data protection laws

3. Processing/Retention Period and Destruction of Personal Information

- **Processing/Retention Period of Personal Information**

  Mandatory information (and optional information, if agreed) set forth above will be retained and used for 6 years from the date of resignation/dismissal, and if necessary under applicable laws and regulations, such personal information may also be retained for a period prescribed by laws and regulations.

  Provided below are examples where we are required to retain your' personal information pursuant to applicable laws and regulations:

  - Register of workers: three (3) years from the date of dismissal, retirement, or death (The Labor Standards Act)
  - Employment agreement: three (3) years from the date on which the employment is terminated (The Labor Standards Act)
  - Documents related to employment, dismissal, and retirement: three (3)

years from the date of dismissal or retirement (The Labor Standards Act)
- Wage ledger: three (3) years from the date on which any matter was recorded therein for the last time (The Labor Standards Act)
- Documents related to recruitment, employment, wage, money and goods other than wages, education assignment, promotion, age limit, retirement and dismissal: three (3) years (Equal Employment Opportunity and Work-Family Balance Assistance Act)
- Documents related to application for, and permits of, childcare leave: three (3) years (Equal Employment Opportunity and Work-Family Balance Assistance Act)
- Documents related to health insurance including management of the eligibility requirements and calculation of insurance premium: three (3) years (National Health Insurance Act)

- **Destruction of Personal Information**

  - When destroying personal information, the Company will take commercially reasonable and technically possible measures to make the personal information irrecoverable or irreproducible as follows:
    - Electronic files which contain personal information will permanently be deleted using a technical method which makes the files irrecoverable; and
    - Any other records, print-outs, documents or any other recording media will be shredded or incinerated.
  - In the event that the processing/retention period has expired, but personal information is required to be retained continuously, the relevant personal information and personal information files will be stored/maintained separately from other personal information, to the extent technically possible.

4. **Provision of Personal Information to a Third Party**

The Company will request Employees to consent in case of providing some or all of Employees' personal information to a third party during the course of employment. The Company may provide some or all of Employees' personal information listed below.

General Personal Information

	Recipient	Provided Items	Recipient's Purposes of Use	Recipient's Period of Retention and Use
Mandatory	OpenAI OpCo LLC	Personal Information mentioned in Section 2	Managing or making decisions in connection with your relationship with your employer or when involved in an HR process concerning your relationship with the your employer (including, without limitation, staff from Compliance, Legal, Employee Relations and Information Security)	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal
	Tax authorities; regulatory authorities; OpenAI's insurers, bankers, and professional advisors; and administrators of the Company's services to employees	Personal Information mentioned in Section 2.	To fulfill OpenAI's legal obligations; to manage or make decisions in connection with your relationship with OpenAI; and to provide us and our employees with services	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal

Unique Identification Information

	Recipient	Provided Items	Recipient's Purposes of Use	Recipient's Period of Retention and Use
Optional	OpenAI OpCo LLC	Unique Identification Information	Managing or making decisions in connection with your relationship with your employer or when involved in an HR process concerning your relationship with the your employer (including, without limitation, staff from Compliance, Legal, Employee Relations and Information Security)	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal
	Tax authorities, regulatory authorities, administrators of the Company's services to employees	Unique Identification Information	To fulfill OpenAI's legal obligations; to manage or make decisions in connection with your relationship with OpenAI; and to provide us and our employees with services	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal

Sensitive Information

	Recipient	Provided Items	Recipient's Purposes of Use	Recipient's Period of Retention and Use

Mandatory	OpenAI OpCo LLC	Personal Information mentioned in Section 2	Managing or making decisions in connection with your relationship with your employer or when involved in an HR process concerning your relationship with the your employer (including, without limitation, staff from Compliance, Legal, Employee Relations and Information Security)	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal

5. Delegation of Processing of Personal Information

The Company will delegate personal information processing tasks as follows, and the delegatee may process personal information according to the purpose of delegation.

Delegatee	Purpose of the Delegated Tasks	Details of Delegation
Staff in OpenAI teams such as the Finance and IT Department and the Global HR information systems support team	Where necessary for the performance of specific tasks or system maintenance	Managing or making decisions in connection with your relationship with your employer or when involved in an HR process concerning your relationship with the your employer (including, without limitation, staff from Compliance, Legal, Employee Relations and Information Security)
Third parties that provide us with services	To provide OpenAI and our employees with services	Hosting, supporting and maintaining the framework of our HR information systems, or providing services on our behalf (for instance payroll provider) to carry out tasks upon our instruction

The Company, when entering into a delegation contract, specifies in the contract or other document the matters concerning the prohibition of processing personal information beyond the scope necessary for the delegation, technical and managerial protective measures, restrictions on re-delegation, supervision and management of the delegatee, and liability for damages in accordance with Article 26 of the PIPA. The Company also supervises whether the delegatee safely processes personal information. In addition, in the event of a change in the content of the delegation or the delegatee, the Company will promptly disclose it through this Privacy Policy.

6. Overseas Transfer of Personal Information

The Company will transfer Employees' personal information overseas as follows. Employees may refuse the overseas transfer of their personal information by contacting the department in charge of protecting personal information and handling employee complaints provided in Section 11 below. Provided, however that

Employees who refuse the overseas transfer of personal information may be subject to personnel and administrative disadvantages.

	Transferee's Name (Contact Information)	**Country where Transferee is Located**	**Transferred Items**	**Transferee's Purposes of Use**	**Time/ Method of Transfer**	**Transferee's Period of Retention and Use**
Mandatory	OpenAI OpCo LLC	United States	Personal Information mentioned in Section 2.	Managing or making decisions in connection with your relationship with the Company or when involved in an HR process concerning your relationship with the Company Performance of specific tasks or system maintenance by staff in OpenAI teams such as the Finance and IT Department and the Global HR information systems support team.	Transmission through the network after consent is obtained and continually thereafter	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal

	Tax authorities; regulatory authorities; OpenAI's insurers, bankers, and professional advisors; and administrators of the Company's services to employees	United States	Personal Information mentioned in Section 2.	To fulfill OpenAI's legal obligations; to manage or make decisions in connection with your relationship with OpenAI; and to provide us and our employees with services	Transmission through the network after consent is obtained and continually thereafter	Unless otherwise obligated to preserve your personal information under applicable laws and regulations, the recipient will retain and use your personal information until the purposes of using the personal information are satisfied but no longer than 6 years from the date of resignation / dismissal

7. Rights and Obligations of Employees and How to Exercise Such Rights

Employees have the right to:

- Request access to their personal information, and to information about how their personal information has been used. This enables Employees to confirm if and how the Company process personal information about Employees and, where that is the case, obtain a copy of the personal information.
- Request rectification of the personal information that the Company holds about Employees. This enables Employees to correct any inaccurate or supplement any incomplete information the Company holds about Employees.
- Withdraw consent to the processing of personal information. When processing is based on consent, Employees have the right to revoke such consent at any time. If Employees ask to withdraw consent, this will not affect any processing which has already taken place at that time.

When requested as above, the Company will check whether the requesting party is the information principal or an authorized representative. The Company may reject such request if there is justifiable reason for rejection under applicable laws or a reason equivalent thereto.

8. Measures to Ensure the Security of Personal Information

G. Managerial measures

- The Company will designate a Chief Privacy Officer ("CPO") to ensure that Employees' personal information is processed according to the law, and

will establish and implement an internal management plan for doing so.

- The Company will establish and implement personal information protection education plans for its Employees, delegatees and others who are directly in charge of processing personal information.
- The Company will require that third parties which may receive personal information go through a diligence process and apply measures to protect the security of any information shared by the Company.
- The Company will take prevention measures by requiring employees to apply appropriate measures to protect the security and confidentiality of personal information. In this event appropriate measures must be taken to protect the confidentiality and integrity of the data during the processing. Once the relevant processing is complete, steps should be taken to store or return the relevant data within the official storage locations/systems with all less formally held records (e.g. local folders, hard copies, emails saved outside of formal managed folders) securely erased.

H. **Technical measures**

(a) The Company will control access to personal information, and will restrict and manage the access right.
(b) The Company will record the details of the management of access to personal information, and will retain such records for a certain period of time.
(c) The Company will install and operate an intrusion blocking/prevention system to prevent any unauthorized access to personal information. In addition, safe access measures, including a virtual private network, will be utilized to control the access from the outside.
(d) The Company will establish and apply password generation rules to enable Employees to set up and use a secure password. Upon designating a password to access information processing system, Employees are obligated to keep the password confidential and must not disclose it to a third party.
(e) At the time of transmitting, receiving and saving personal information, including sensitive information and unique ID information, the Company will take encryption measures required under applicable laws and regulations.
(f) The Company will install and periodically update programs to fix security defects in software, including operating systems and take technical data security measures such as protected server environment, firewalls and SSL encryption.
(g) The Company will keep the records of access to the personal information processing system in a safe manner for a certain period of time.

I. **Physical measures**

The Company will take physical access prevention measures, including restrictions on access and placing locks, to store personal information kept by way of hard copy in a safe manner as below:

1) If employees are in possession of personal data of any kind (e.g., data collected in emails, address books, Excel spreadsheets or contained in curricula vitae or elsewhere), they must ensure that the data are kept in a safe place where unauthorized access cannot occur. Where data is retained in hard copy, storage in a locked drawer or cabinet, accessible only to authorized individuals, is generally the most effective means of securing the data.

9. Criteria for Additional Use or Provision of Personal Information to a Third Party

According to Articles 15 (3) and 17 (4) of the amended PIPA, the personal information controller may additionally use and provide personal information to a third party without the data subject's consent in consideration of the matters prescribed in Article 14-2 of the Enforcement Decree of the PIPA:

1) the purpose of additional use and provision is substantially related to the original purpose for which the personal information was collected;

2) the additional use and provision is foreseeable in light of the circumstances and practices;

3) the additional use and provision does not unfairly infringe on the interests of the data subject; and

4) whether necessary security measures such as pseudonymization or encryption have been taken.

10. Remedy for Infringement on Rights

If Employees need to report or consult on any personal information infringement, please contact the following institutions.

1) Personal Information Dispute Mediation Committee: 1833-6972 (www.kopico.go.kr)
2) Korea Internet & Security Agency's Personal Information Infringement Reporting Center: 118 (privacy.kisa.or.kr)
3) High-tech Crime Investigation Division of the Supreme Prosecutors' Office: 1301 (www.spo.go.kr)
4) Cyber-Terrorism Response Center of the National Police Agency: 182 (ecrm.cyber.go.kr)

11. Department in charge of Protecting Personal Information and Handling Employee Complaints

The Company’s HR Department will be in charge of protecting Employees’ personal information and handling complaints related to their personal information. Employees may file any complaints related to protection of their personal

information which may arise during employment period to the Privacy Department at the following contact.

Department:	HR
Contact Information:	hr@openai.com

12. **Enactment and Amendments to this Privacy Policy**

This Privacy Policy was enacted and effective on July 1, 2025 and will remain effective unless otherwise noted. If there are any additions, deletions, or modifications due to changes in laws, policies, or security technologies, the revised Privacy Policy will be provided to you, along with the reasons and details for the changes.

JAPAN Additional Clauses Applicable to Employees, Applicants and Candidates Special Categories of Personal Data

The special categories of personal data of you and your family member that may be processed by us are set out in this Privacy Notice. We will obtain your consent to collect special categories of personal data. You shall ensure to obtain consent upon providing the special categories of personal data of your family members to us.

International data transfer

Due to the global nature of our operations, we may transfer or disclose your personal data to personnel, servers or organizations outside of Japan, including the United States, Canada, the UK, and Ireland. Where we share your personal information, we will put in place contractual measures to ensure they process your personal data in accordance with our instructions and have in place technical and organizational measures to protect your personal data with a level of protection comparable to that required under the Act on the Protection of Personal Information ("APPI").

Data Subject Rights

In Japan, you have rights under the APPI such as:

- the right to access to, or obtain a copy of your personal data;
- the right to request deletion or cessation of processing of your personal data if your personal data has been used beyond the scope necessary to achieve the purpose(s) for which they were collected, processed or obtained by deceit or in violation of the APPI, if our use of your personal data triggers illegal acts, is no longer necessary in relation to the purposes for which they were collected, compromised or otherwise processed in a manner which could harm the rights or legitimate interest of you;
- the right to request cessation of transferring of your personal data if your personal data is transferred to a third party in violation of the APPI or the transfer could harm your rights or legitimate interest;
- the right to request disclosure of the following information (we may refuse your request to the extent we are permitted to do so in accordance with APPI):
    - data security measures we have implemented; and
    - in case where your personal data has been shared with foreign companies including our subsidiaries and affiliates and external foreign service providers, (i) measures to ensure the data recipients take sufficient data security measures (the "Measures") and the details of the Measures, (ii) measures and frequency that we audit the data recipients' implementation of the Measures, (iii) name of the recipient country and rules of the country that could hinder the implementation of the Measures, and (iv) other obstacles that could hinder the implementation of the Measures and measures that we have conducted to solve such obstacles.

Processing of My Numbers

We may directly obtain from you and process your (including your family member's) Individual Number prescribed in Article 2 (5) of Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (the "My Number Act") ("Individual Number") for the purpose of tax, social insurance or disaster recovery purposes in accordance with the My Number Act and other relevant laws and regulations.

Contact Information

If you have any complaints regarding our processing of your personal data, questions on this Privacy Notice, our use of your personal data, international transfer or our data protection measures implemented, and/or want to confirm the measures to exercise your privacy rights above, please contact hrprivacy@openai.com.

SINGAPORE Additional Clauses Applicable to Employees, Interns, Secondees and Applicants

In Singapore, you have specific rights under the Personal Data Protection Act (2012):

- You have the right to request access to any of your personal data that was used or disclosed within a year before your request. You may also request correction of any inaccurate data relating to you. The Company aims to ensure that all personal data are correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to the Company so that we can ensure that your data is up-to-date. You can see and update some of this data yourself via your applicable HR system account. However, to correct/update certain information, you will need to contact hr@openai.com.
- We will cease to retain your personal data or dispose of it in a proper manner when it is no longer needed for any business or legal purpose.
- Due to the global nature of our operations, we may transfer or disclose your personal data to personnel, servers, OpenAI entities and managers, and service providers outside of Singapore, including the United States, Canada, Japan, the UK, and Ireland. Where we share your personal data, we will put in place contractual measures to ensure recipients process your personal data in accordance with our instructions and have in place technical and organizational measures to protect your personal data with a level of protection comparable to the protection under Singapore's Personal Data Protection Act.
- We will notify you of any data breach that is or is likely to be of significant scale, or results in or is likely to result in significant harm to you.
- At your request, we will transmit your personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. Our Data Protection Officer ("DPO") is responsible for compliance with personal data protection law. Please contact our DPO (hrprivacy@openai.com, please put in the subject line, "Attention: DPO") at any time if you have any concerns about the processing of your personal data or any data protection issue. If you have any questions regarding the processing of your personal data or if you believe your privacy rights have been violated, please contact your local Human Resources contact hr@openai.com or, where applicable, the DPO. If you are aware of an unauthorised disclosure of data, please report this immediately to hrprivacy@openai.com.

CONSENT LANGUAGE FOR SINGAPORE

By signing below, I acknowledge and consent to my personal data (including sensitive personal data such as social security number, passport number, medical information etc.) to be collected, used, transferred and processed by the Company and OpenAI.

I also consent to the Company's and OpenAI's sharing of my personal data with third parties for purposes described in this Global Data Privacy Notice for Employees, Applicants and Candidates.

Signature: _____

Name:_____

Date: _____

AUSTRALIA Additional Information for Employees, Applicants, Contractors

This information supplements the above policy and applies to employees and contractors engaged by OpenAI Australia Pty. Ltd. as well as persons applying for a position with that company.

Subject to applicable law, you have the right to access and correct your Personal Data.

Your Personal Data may be transferred to recipients located in the United States.

If you are concerned about how we have handled your Personal Data, you may contact the Office of the Australian Information Commissioner (www.oaic.gov.au).

INDIA Additional Data Privacy Notice Applicable to Staff Personnel

Additional Categories of Personal Data

In India, we may seek the following additional categories of personal data from you:

Type of Personal Data	Purpose
Government issued identity documents such as Aadhaar card, PAN card, voter identity card, etc.	To conduct background and identity verification. To fulfil know-your-customer (KYC) and regulatory compliance requirements, where required. To facilitate your registration for employee benefits and retirement-related entitlements.
Passwords	To authenticate your identity and grant you access to our systems. To record your attendance and participation. To improve the security of our systems and services.

Your Rights

In India, subject to the conditions and limitations set forth under applicable laws, you have the following specific rights in respect of your personal data:

Right	Description
Right to access your personal data	Where we have relied on your consent to process your personal data, or where you have voluntarily provided your personal data for a specified purpose, you have the right to obtain information from us as below: (h) Summary of personal data and processing activities: You have the right to receive a summary of the personal data that is being processed by us, along with details regarding the processing activities undertaken by us with respect to such personal data. (i) Identities of other entities: You have the right to know the identities of all other entities with whom your personal data has been shared by us. This includes a description of the personal data shared with these entities.
Right to correct, complete and update your personal data	Where we have relied on your consent to process your personal data, or where you have voluntarily provided your personal data for a specified purpose, you have the following rights in respect of your personal data: (a) Correct any inaccurate or misleading personal data. (b) Complete the incomplete personal data. (c) Update your personal data If you are an employee, you can see and update some of this data yourself via your applicable HR system account. However, to correct / complete / update certain information, you will need to reach out to us in accordance with the process mentioned below.
Right to request for erasure of personal data	Where we have relied on consent to process your personal data, or where you have voluntarily provided your personal data for a specified purpose, you have the right to request for the erasure / deletion of your personal data under certain circumstances, such as when the personal data is no longer necessary for the purposes for which it was collected or there is no statutory obligation to retain such personal data.

Right to withdraw consent	Where we have relied on your consent to process your personal data, you have the right to withdraw your consent. Please note that withdrawal of your consent will not be retrospective in nature and shall be applicable prospectively. Further, you will be responsible for any consequences of withdrawal of your consent, but such withdrawal of consent will not affect the legality of any personal data processing done by us based on your consent before it was withdrawn. Please note that the withdrawal of consent or exercise of right to erasure may impact our ability to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations, such that withdrawal of consent or exercise of right to erasure may impact our ability to provide continued employment.
Right to grievance redressal	You have the right to readily available grievance redressal regarding our processing of your personal data, including the exercise of your rights in relation to such personal data.
Right to nominate	You have the right to nominate any other person to exercise the rights available to you under this India Data Privacy Notice, in case of your death or incapacity.

How To Exercise Your Rights

Unless a specific mechanism for exercising a certain right has already been mentioned above, you may exercise your rights by contacting us using either method below:

(a) Send an email to: hr@openai.com; or
(b) Call us at: 1 (844) 534-9165

When submitting a request for exercise of your rights, we may require additional information from you, such as your employee ID or other registration number that uniquely identifies you or take other steps to verify your identity. We may decline to process requests that are frivolous or unreasonably repetitive or burdensome, risk the privacy or impact the rights of others, or are extremely impractical.

Contact

If you have any queries or issues in relation to processing of your personal data or regarding exercise of your rights under this India Data Privacy Notice, you may contact the Company's Grievance Officer / Data Protection Officer ("DPO"). The DPO can be reached at hrprivacy@openai.com (please put in your subject line, "Attention: DPO").

We will endeavour to respond to your requests within 30 days. However, if additional time is required due to the nature of the request or query, we will keep you appropriately informed.

If you would like to access the Privacy Notice, including the India Data Privacy Notice in any of the following languages - Assamese, Bengali, Bodo, Dogri, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Mathilli, Malayalam, Manipuri, Marathi, Nepali, Odia, Punjabi, Sanskrit, Santhali, Sindhi, Tamil, Telugu and Urdu - please contact us at hr@openai.com.

UNITED ARAB EMIRATES (ADGM) - Additional Information for Staff

Data Controller

OpenAI MENA Limited to which you submit an application for employment or with which you have your contract (the “Company”) and OpenAI OpCo, LLC act as joint controllers of your personal data, which means the Company and OpenAI OpCo, LLC jointly determine how to use your personal data in connection with your application and employment (but only as described in this Data Privacy Notice).

This Data Privacy Notice applies to the processing of your personal data by both the Company and OpenAI OpCo, LLC, and references in this notice to the 'Company' (including 'we', 'our' or 'us') shall, where applicable, be deemed to include a reference to both the Company and OpenAI OpCo, LLC. The Company will be primarily responsible for providing you with any information to which you are entitled, and responding to your requests, under data protection law.

Contacts

You may contact the Company’s Data Protection Officer (“DPO”) at any time if you have any concerns about the processing of your personal data or any data protection issue. The DPO can be reached at hrprivacy@openai.com (please put in your subject line, “Attention: DPO”).

If you have any questions regarding the processing of your personal data or if you believe your privacy rights have been violated, please contact your local Human Resources contact hr@OpenAI.com or, where applicable, the DPO. If you are aware of an unauthorised disclosure of data, please report this immediately to hrprivacy@openai.com.
LEGAL BASES FOR PROCESSING

Personal data

Whenever the Company and OpenAI OpCo, LLC process your personal data, we do so on the basis of a lawful condition (“legal basis”) for processing. Processing of special categories of data is always justified on the basis of an additional condition.

In the majority of cases, the processing of your personal data will be justified on one of the following legal bases:

- the processing is necessary for compliance with a legal obligation to which the Company is subject (for example, disclosing the information to tax authorities, making statutory payments, avoiding unlawful termination, avoiding unlawful discrimination, meeting statutory record keeping requirements or health and safety obligations);
- where there is no legal obligation, we will process your data where the processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into such a contract (for example, collecting bank details to pay your salary or processing information to provide you with the contractual benefits you are entitled to); or
- where the above two grounds do not apply, we may process your personal data where the processing is necessary for the legitimate interests pursued by the Company (being those purposes described in Section 3 of the Data Privacy Notice), except where such interests are overridden by your interests or fundamental rights and freedoms (for example, reviewing your performance at work).

We will, on occasion, process your personal data where it is necessary for the legitimate interests pursued by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms.

In exceptional circumstances, where we have no legitimate interest in processing but you ask us to process data for a particular purpose, we will occasionally carry out the processing on the basis of your consent (for example, if you ask us to provide pay information to a bank for a mortgage application made by you). Where we rely on your consent, we will make this clear at the relevant time to you.

Special categories of data

The special categories of personal data that may be processed by the Company are set out in this Data Privacy Notice. Where we process special categories of data, it will be justified by a legal basis set out above and also by one of the following additional conditions:

- the processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, to the extent permissible under applicable laws;
- the processing is necessary for health purposes, including preventative or occupational medicine, for the assessment of your working capacity, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems and services, or pursuant to a contract with a health professional provided that processing is by or under the responsibility of a health professional subject to the obligation of professional secrecy or duty of confidentiality, to the extent permitted by applicable laws;
- the processing is necessary to protect your vital interests or the vital interests of another person where you are physically or legally incapable of giving consent (for example, in exceptional emergency situations, such as a medical emergency);
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest, to the extent permissible under applicable laws; or
- In exceptional circumstances, the processing is carried out subject to your explicit consent (as explained below).

We will occasionally seek your consent to certain processing which is not otherwise justified under one of the above conditions. If consent is required for the processing in question, it will be sought from you separately to ensure that it is freely-given, informed and explicit. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any such consent. You should be aware that it is not a condition or requirement of your employment to agree to any request for consent from the Company.

Transfers of Personal Data Outside the Abu Dhabi Global Market ("ADGM")

From time to time, your personal data (including special categories of personal data) will be transferred to OpenAI entities to process for the purposes described in this Data Privacy Notice. This will be applicable for example where the relevant entity or a manager from that entity is responsible for conducting or approving the relevant process or the data is part of a global directory where other individuals need to have access.

These entities or managers may be located outside the ADGM, including within the European Economic Area (EEA), United Kingdom, Switzerland and elsewhere in the world (for example, OpenAI OpCo, LLC based in the United States).

Personal data may also be transferred to third parties (e.g., service providers or regulators as set out above), who may have systems or suppliers located outside the ADGM. As a result, in some

circumstances your personal data will be transferred to jurisdictions outside of the ADGM whose data protection laws may be less stringent than those applicable in the ADGM.

We may transfer your personal data to jurisdictions outside of the ADGM, provided that:

a) such jurisdictions provide for an adequate level of data protection according to the assessment of the ADGM Commissioner of Data Protection ("Adequacy Decision", e.g. pursuant Art. 41 ADGM Data Protection Regulations 2021[3]),

b) the Company ensures that appropriate or suitable safeguards are in place to protect your personal data and that transfer of your personal data is in compliance with applicable data protection laws (e.g., Art. 42 ADGM Data Protection Regulations 2021), or

c) we may rely on a statutory derogation (e.g., Art. 44 ADGM Data Protection Regulations 2021).

The countries to which your personal data may be transferred are: countries within the EEA, the United Kingdom, Switzerland, and the United States.

Where required by applicable data protection laws, in particular because there is no Adequacy Decision, the Company has ensured that service providers (including other OpenAI group entities) sign standard contractual clauses approved by the ADGM Commissioner of Data Protection (Art. 42 ADGM Data Protection Regulations 2021) to ensure that appropriate safeguards are in place and enforceable rights and effective legal remedies are available to you. You can obtain a copy of any standard contractual clauses in place, and any other implemented appropriate safeguards which relate to transfers of your personal data, by contacting hrprivacy@openai.com. Please note that such copy may be redacted to the extent necessary to protect business secrets or other confidential information.

OpenAI has an intra-group data transfer agreement in place which regulates cross-border transfers of your data within the OpenAI group.

YOUR RIGHTS AS A DATA SUBJECT

Subject to the conditions and limitations set forth in the ADGM Data Protection Regulations 2021, you have the following rights in respect of your personal data.

Right	Description

[3] A list of the Commissioner of Data Protection's adequacy decisions can be found here.

Right to access, correct and delete your personal data	The Company aims to ensure that all personal data are correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to the Company so that we can ensure that your data is up-to-date. You have the right to request access to any of your personal data that the Company may hold, and to request correction of any inaccurate data relating to you or the completion of any incomplete personal data. You furthermore have the right to request deletion of any irrelevant data we hold about you. If you are an employee, you can see and update some of this data yourself via your applicable HR system account. However, to correct / update certain information, you will need to contact hr@openai.com.
Data portability	Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to the Company in a structured, commonly-used and machine-readable format, and also to require us to transmit it to another controller where this is technically feasible.
Right to restriction of processing	You have the right to restrict our processing of your personal data where: ● you contest the accuracy of the personal data, until we have taken sufficient steps to correct or verify its accuracy; ● where the processing is unlawful but you do not want us to erase the data; ● where we no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims; or ● where you have objected to processing justified on legitimate interest grounds (see below), pending verification as to whether the Company has compelling legitimate grounds to continue processing. Where personal data is subjected to restriction in this way, we will only process it with your consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest.
Right to withdraw consent	Where you have provided us with your consent to process particular personal data, you have the right to withdraw such consent at any time. You can do this by: ● in some cases, deleting the relevant data from the relevant HR system (although note that in this case it may remain in back-ups and linked systems until it is deleted in accordance with our data retention policy); or ● contacting your local Human Resources contact. It will only, however, be rare that we rely on your consent to process personal data for your employment or engagement.

Right to object to processing justified on legitimate interest grounds	Where we are relying upon legitimate interest to process personal data, then you have the right to object to that processing. If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims. Where we rely upon legitimate interest as a basis for processing, we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.
Right to complain	You also have the right to lodge a complaint with the ADGM Commissioner of Data Protection if you consider that the processing of your personal data infringes the Abu Dhabi Data Protection Regulations 2021. We request that you contact us in the first instance to allow us to remedy any complaints.

BRAZIL DATA PRIVACY NOTICE

Data Controller

The OpenAI entity to which you submit an application for employment or with which you have your contract (the "Company") acts as the controller of your personal data, determining how to use your personal data in connection with your application and employment - but only as described in this Data Privacy Notice. The Company will be primarily responsible for providing you with any information to which you are entitled, and responding to your requests, under data protection law.

Contacts

You may contact the Company's Data Protection Officer ("DPO") at any time if you have any concerns about the processing of your personal data or any data protection issue. The DPO can be reached at hrprivacy@openai.com (please put in your subject line, "Attention: DPO").

LEGAL BASES FOR PROCESSING

Personal data

Whenever the Company processes your personal data, we do so based on a legal basis for processing. In the majority of cases, the processing of your personal data will be justified on one of the following bases:

- where the processing is **necessary for compliance with a legal obligation** to which the Company is subject (for example, disclosing the information to tax authorities, making statutory payments, avoiding unlawful termination, avoiding unlawful discrimination, meeting statutory record keeping requirements or health and safety obligations);
- where the processing is **necessary for the performance of a contract** to which you are a party or in order to take steps at your request prior to entering into such a contract (for example collecting bank details to pay your salary or processing information to provide you with the contractual benefits you are entitled to);
- where the processing is necessary for the **legitimate interests pursued by the Company** (being those purposes described in the section 3.0 of the main policy), except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data (for example reviewing your performance at work); or
- where the processing is necessary for the **regular exercise of Company's rights** in administrative, judicial or arbitration proceedings (for example, to defend the Company in case a lawsuit is filed).

We will on occasion process your personal data for the purpose of legitimate interests pursued by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data.

In exceptional circumstances we will carry out the processing on the basis of your consent (for example if you ask us to provide pay information to a bank for a mortgage application made by you). Where we rely on your consent, we will make this clear at the relevant time to you.

Sensitive personal data

Sensitive personal data that may be processed by the Company is set out in this Data Privacy Notice. Where we process sensitive personal data, it will be justified on a legal basis, such as:

- where you have provided your specific and highlighted consent for specific purposes;

- where the processing is necessary for compliance with a legal obligation to which the Company is subject;
- where the processing is necessary for the regular exercise of Company's rights in administrative, judicial or arbitration proceedings; or
- where the processing is necessary for protection of your life or safety or of a third party's.

If consent is required for a processing, it will be sought from you separately to ensure that it is freely given, informed and unambiguous. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any such consent. You should be aware that it is not a condition or requirement of your employment to agree to any request for consent from the Company.

INTERNATIONAL TRANSFER OF PERSONAL DATA

From time to time your personal data (including sensitive personal data) will be transferred to OpenAI entities to process for the purposes described in this Data Privacy Notice. This will be applicable for example where the relevant entity or a manager from that entity is responsible for conducting or approving the relevant process or the data is part of a global directory where other individuals need to have access.

These entities or managers are located within the United States.

Personal data may also be transferred to third parties (e.g. service providers or regulators as set out above), who may have systems or suppliers located outside Brazil. As a result, in some circumstances your personal data will be transferred to countries outside of Brazil to countries whose data protection laws may be less stringent than the Brazilian General Data Protection Law ("LGPD"). In that case, the Company will provide an adequate level of protection of your personal data, including by entering into appropriate contractual terms with recipients of personal data.

OpenAI has an intra-group data transfer agreement in place which regulates cross-border transfers of your data within the OpenAI group.

Please find below consolidated information on the international transfers of personal data that we may carry out:

- Form, Duration and Specific Purpose of the International Transfer: We may transfer personal information relating to you from Brazil via private digital communication networks, for the purposes described in Section 3.0, and your Personal Data will be retained in relation to the international transfer for as long as it is necessary to fulfill such purposes, unless retention is required for compliance with legal or regulatory requirements.
- Country of Destination: Your Personal Data may be accessed in the United States.
- Identification of the controller: See the item "Data Controller" above.
- The shared used and the purpose of sharing: See purposes described in Section 4.0.
- The responsibilities of the processing agents and the security measures adopted: the Data Controller shall be responsible for (i) publishing information on the international transfer; (ii) responding to data subjects' requests; and (iii) notifying ANPD and data subjects of security incidents which may cause significant risk or damage to data subjects. See security measures described in Section 5.0.
- The rights of the data subject and the means of exercising them: See the following Section.

YOUR RIGHTS AS A DATA SUBJECT

Subject to the conditions and limitations set forth in LGPD, you have the following rights in respect of your personal data.

Right	Description
Right of confirmation and access	You have the right to obtain confirmation as to whether the Company is processing your personal data, and to request access to any of your personal data that the Company may hold. You also have the right to obtain information about the processing of your personal data, including information regarding the public and private entities with which the Company shares your personal data If you are an employee, you can see and update some of this data yourself via your applicable HR system account. However, to correct / update certain information, you will need to contact hr@openai.com.
Right to correct your personal data	You have the right to request correction of any inaccurate data relating to you, as well as to complete any incomplete or update any outdated personal data that the Company holds. The Company aims to ensure that all personal data is correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to the Company so that we can ensure that your data is up-to-date.
Right to anonymization, blocking or erasure	You have the right, in some circumstances, to require the Company to anonymize, block or erase personal data concerning you, e.g., where personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, where consent is withdrawn and there is no other legal basis for processing, or where personal data is unlawfully processed. The right to erasure does not apply in certain circumstances, including where the processing is necessary for the establishment, exercise, or defense of legal claims.
Data portability	You have the right to request that the personal data concerning you is transmitted to another service or product provider, limited to the Company's commercial or industrial secrets.
Right to withdraw consent	Where we have relied on your consent to process particular information and you have provided us with your consent to process data, you have the right to withdraw such consent at any time. You also have the right to request the erasure of personal data concerning you once consent is

	withdrawn and to be informed about the possibility of denying consent, and the consequences of such denial. We may, however, have other legal grounds to continue to process the personal data for other purposes.
Right to object	You have the right to object to any processing of personal data to the extent that the Company relies on legal bases other than your consent, in case of violation of the LGPD.
Right to revision	You have the right to request the revision of decisions taken solely on the basis of automated processing of your personal data which affects your interests, including decisions intended to define personal, professional, consumer or credit profile or aspects of your personality.
Right to complain	You also have the right to lodge a complaint with the supervisory authority if you consider that the processing of your personal data infringes the LGPD provisions. We would request that you contact us in the first instance to allow us to remedy any complaints.