**CALIFORNIA cONSUMER pRIVACY aCT nOTICE**

This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS applies solely to employees, consultants and applicants for employment of General Dynamics Information Technology, Inc. and its subsidiaries and managed affiliates, who reside in the State of California. We adopt this notice to comply with the California Consumer Privacy Act of 2018 (“CCPA”) as modified by the California Privacy Rights Act of 2020 (collectively, the “CPRA”), and other California privacy laws.  Any terms defined in the CPRA have the same meaning when used in this notice.

**Personal Information GDIT Collects**

The CCPA and CPRA define “Personal information” as information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Under the CPRA, “Personal Information” further includes “Sensitive Personal Information” such as social security number, driver’s license number, state identification card, passport number, certain financial account data, genetic data, certain biometric data, precise geolocation, racial and ethnic origin, content of consumer communications (email, mail, or text), unless the business is the intended recipient, and information collected concerning a consumer’s health, sex life, or sexual orientation.

Below are the categories of Personal Information that we may have collected or shared for a business purpose in the last twelve (12) months, as permitted by law:

|  |  |
| --- | --- |
| **Category** | **Examples** |
| Identifiers | A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number\*, driver’s license number\*, passport number\*, or other similar identifiers. |
| Personal Information | Your identity: to include last name, first name, maiden name; date of birth; sex; race/ethnicity\*; home address; home telephone number; home email, name and telephone number of a contact in case of emergency; passport number\* and related materials for processing of residency or other immigration status (if applicable); driver's license number\* (if applicable); work permit number; social security number\* (if applicable and only as required for payroll, benefit, insurance, and work eligibility purposes); other identification document numbers (if applicable) provided for work eligibility purposes; country of birth and nationality\* (if applicable); bank account details\*; employee identification number; and, if any, your disability rate\* (if applicable) as required for GDIT to comply with its legal duty; your disability\* and veteran status (if applicable); marriage certificates and banking loan information\* for processing for relocation matters; and personal banking information\* for processing of payroll.Family status: to include marital status; last name, first name and date of birth of your spouse or partner (should you and your spouse or partner wish to be added to your insurance); last name, first name, and date of birth of your children (should you wish to add them to your insurance); last name, first name, and date of birth for any designated beneficiaries; insurance information; retirement account information |
| Protected classification characteristics under California or federal law | Age (40 years or older), race\*, color\*, ancestry\*, 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\*, veteran or military status, genetic information\* (including familial genetic information). Some personal information included in this category may overlap with other categories. |
| Internet or other similar network activity | Information may be automatically collected by our website, including your IP address, the address of the site you visited just prior to ours, and number of times an article or page from our site has been shared.  |
| Geolocation | Information identifying your physical location or movements |
| Sensory data | Audio, electronic, visual, thermal, olfactory, or similar information. |
| Education Information | Education and development: to include diplomas and training certificates held; languages and proficiency (if applicable); curriculum vitae detailing your work experience and if applicable, military experience (but not the reasons for deferment or rejection from the military service, if any); continuous training; mobility situation and management of career development actions; performance evaluations; training programs completed.  |
| Professional and employment-related information | Employment terms and conditions: employment status; to include fixed-term contract or open-ended contract (if applicable); part-time or full-time job; hire date; termination date; division; department; reporting structure; job title; pay grade; work telephone number and work email address; job description; salary schedule and other compensation elements; participation in and elements of awards under the executive compensation plan, if applicable; related payments; actual working hours or shift time; retirement fund contribution; tax and source tax deductions; absence management (in particular sick leave, leave of absence, family leave, parental leave); paid holidays (if applicable); time off given in compensation for extra time worked); personnel representative status.  |

\*Denotes Sensitive Personal Information as defined by CPRA.

For purposes of this notice, Personal information does not include:

• Publicly available information such as from government records or information made available to the general public.

• De-identified or aggregated consumer information.

• Information excluded from the CPRA’s scope, such as: (i) Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or ii) Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

**Sources of Personal Information**

We collect personal information you voluntarily provide to us during the application process, onboarding process, through our administration of payroll, benefits, and other employment functions, and when you otherwise contact us. We may also automatically collect certain information, such as IP addresses and device identifiers.

We may combine personal information you voluntarily provide to us with information we collect from other sources, such as:

* Recruiters;
* Prior employers and professional references;
* Educational institutions;
* Pre-employment screening and background check services;
* Credentialing and licensing organizations;
* Publicly available sources, such as public social media profiles on LinkedIn, Twitter or Facebook; and
* Other sources as provided by you

**Purposes For Which Personal Information Will Be Used**

We use your personal information to help ensure effective personnel administration, including for the following purposes:

* Salary and Benefits. Personal information is used to administer the salaries, benefits, and insurance that you receive under your employment agreement, including annual merit increases, any other salary adjustments, annual bonus payments and retirement plan management, including other benefits provided to retirees; income tax; and social security withholdings.
* Security: Some of your personal information is collected and processed for security purposes including office access and IT resources access. Personal information may be collected in the course of IT resources security procedures, including security penetration tests, for which IT experts will try to access our system to find any security breaches.
* General Management and Human Resources Administration: Personal information may also be used for administration purposes, including employee feedback through the use of employee surveys and contacting employees; administration of email systems and company directories; assignment of offices and other Company equipment; assignment of identification badges; and evaluations performed for purposes such as headcount, diversity and inclusion measures and overall corporate programs to promote an optimal workplace. Personal information may also be used for GDIT’s planning and budgeting; financial reporting; corporate reorganizations; outsourcing; restructuring; and acquisitions and divestments. Personal information may also be used for human resources administration such as to obtain feedback from personnel about GDIT and the work-life environment, so as to identify areas where the organization can improve and related matters.
* Monitoring: We will only monitor your use of GDIT IT Resources in accordance with applicable statutory requirements (including, if applicable, notification of relevant authorities).
* Performance in Your Job within GDIT: To assign a workspace, office, computers, other GDIT equipment, to keep track of the individuals to whom the equipment is assigned, and to enable access to GDIT’s IT systems and applications, including third party applications used to perform your job.
* Travel Arrangements and Business Expense Processing: Personal information is used to make travel arrangements and to process business expenses associated with business travel; to process business expenses associated with approved coursework, books and periodicals, and training; to process business expenses associated with approved business
* Performance Review and Management: GDIT uses personal information to facilitate personnel performance management and career development, notably through annual performance appraisals; annual salary reviews, and; if any, disciplinary measures in accordance with local legislation
* Legal Obligations: We use your personal information to comply with our legal obligations, such as income tax and social security withholdings; disability and family leave obligations; or cooperation with courts, including civil actions, and with law enforcement agencies in legal investigations regarding suspected criminal activities or other suspected illegal activities. GDIT may also use your personal information to comply with federal, state and local contracting and reporting obligations. Subject to local law requirements, GDIT may use your personal information to protect our legal rights or support any claim, defense or declaration in a case or before any jurisdictional and/or administrative authority or arbitration or mediation panel, in the context of disciplinary actions/investigations or of internal or external audit and inquiries.
* Reporting: Personal information may be collected through the compliance hotline implemented by General Dynamics Corporation as a means of allowing employees to report allegations related to the following matters, or other areas of concern: accounting, internal accounting controls, auditing matters, bribery, banking and financial crime; facts affecting the vital interest of GDIT; or issues related to employees’ physical or moral integrity. The collected personal information may be transferred to General Dynamics Corporation located in Falls Church, Virginia USA in the event that the message received through the reporting system may affect substantially the legitimate interests of General Dynamics Corporation, GDIT or any of their affiliates.

We may also use your Personal Information to:

* Verify or maintain the quality or safety of services owned, manufactured, or controlled by us
* Comply with applicable laws or legal process, including court order or subpoena
* Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons
* Cooperate with law enforcement agencies regarding conduct that we reasonably and in good faith believe may violate applicable law
* Cooperate with government agencies in an emergency situation where an employee may be at risk of serious physical injury or death
* Exercise or defend legal claims

We retain your Personal Information for the period reasonably necessary to provide these goods and services to you, such as the term of your employment, and for the period reasonably necessary to support our business operational purposes listed above. We retain records consistent with our record retention policy, including appropriate disposal at the end of applicable retention periods.

**Personal Information We May Disclose**

We may disclose the Personal Information described above with service providers that assist us in providing the services and goods described in this policy. These service providers include payroll processing providers, background check providers, benefits administrators, health insurance providers, travel providers and credit card issuers.

We do not sell or share personal information as defined in the CCPA or CPRA.

**Your Rights and Choices**

The CPRA provides California residents with specific rights regarding their personal information. This section describes your privacy rights and explains how to exercise those rights.

***Access to Specific Information and Data Portability Rights***

You have the right to request that we disclose certain information to you about our collection and use of your personal and sensitive information unless responding to the request is impossible or involves disproportionate effort. Once we receive and confirm your verifiable request, we will disclose to you:

* The categories of personal information and sensitive information we collected about you.
* The categories of sources for the personal and sensitive information we collected about you.
* Our business or commercial purpose for collecting, using and/or disclosing that information.
* The categories of third parties, contractors and service providers with whom we disclose that personal information.
* The specific pieces of personal information we collected about you in a readily useable format (also called a data portability request).
* If we disclosed your personal information for a business purpose, a list of those disclosures, identifying the personal information categories that each category of recipient obtained.
* Whether your information is sold or shared.
* The retention period or criteria used for retention.

***Correction Request Rights***

You have the right to request that we correct any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable request, we will correct (and direct our service providers to correct) your personal information from our records, unless an exception applies. We will evaluate your request based on the totality of the circumstances, including the nature of the personal information, how we obtained it, and any documentation relating to the accuracy of the information. We may deny your request if we determine that the information is more likely accurate than not based on this evaluation. We may opt to delete your personal information instead of correcting it if the deletion will not negatively impact you or you provide your consent.

***Deletion Request Rights***

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

* Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
* Help to ensure security and integrity to the extent the use of the consumer’s personal information is reasonably necessary and proportionate for those purposes.
* Debug products to identify and repair errors that impair existing intended functionality.
* Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
* Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
* Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
* Comply with a legal obligation.

***Exercising Access, Data Portability, Correction, and Deletion Rights***

If you are a California resident not covered by an applicable exclusion and you would like to exercise your rights, you should contact GDIT either by calling 1-800-242-0230 (request Don Creston, Legal Dept.) or emailing us at privacy@GDIT.com. Please provide your name, a way for GDIT to contact you (such as an email address or telephone number) so that we can respond to your request, information about the nature of your relationship with us (for example, are you an employee or a visitor to our website), and details about the action that you would like us to take. Based on your request, we will investigate to determine if we have any of your personal information. If we do have your personal information (other than that provided in your request), we will seek to verify your identity based on the personal information that we already have; the data we will request will depend on the nature of the personal information we have about you. Once we verify your identity, we will provide you with a response, indicating how we will satisfy your request or why we cannot comply with your request.

***Response Timing and Format***

We endeavor to respond to a verifiable request within forty-five (45) days of its receipt. If we require more time, we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the verifiable request’s receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

***Personal Information Sales Opt-Out and Opt-In Rights***

GDIT does not sell or share your personal information as defined under CCPA and CPRA.

***Non-Discrimination***

We will not discriminate against you for exercising any of your California privacy rights.

**Changes To Notice**

GDIT may make changes to this Notice. Notification of changes will be posted on GDIT.com. You should review this Notice periodically to keep up to date on our most current policies and practices.

Date of last update:  December 31, 2022

**Questions And Contact Information**

If you have questions regarding this Notice, please contact the GDIT Privacy Office at privacy@GDIT.com