Proud history, bright future.

Corporate Policy

Process Owner: General Counsel
Content Owner: Director, Global Labor and Employment Law

Global Data Privacy

Date: **October 11, 2021** **Reference No:** **P-GL-KBR-LL-1012**

PURPOSE:

KBR, Inc. ("KBR" or the "Company") is dedicated to conducting business lawfully and ethically. This Policy establishes appropriate, worldwide standards for data protection (privacy) and security of the Personal and Sensitive Personal Data (defined below and collectively referred to in this Policy as "Personal Data") that we collect and process. In particular, our privacy standards are designed to be consistent with applicable laws and requirements and, as appropriate, to also take into account and comply with any notices and contracts or other agreements entered into with individuals or entities in relation to Personal Data.

SCOPE:

This Policy applies to the collection, processing and storage of Personal Data by the Company including that relating to our employees, customers, suppliers, contractors, service providers, contractual partners, affiliates, subsidiaries and other parties, regardless of the origin of the information or the format in which it is contained. All Company employees, contractors, and suppliers worldwide who access Personal Data are required to comply with this Policy.

Third parties with which the Company shares Personal Data must also ensure that they comply with this Policy or one that is substantially similar.

POLICY:

As a global organization, the Company has established a privacy and security framework that is designed to address international, national and local requirements for data privacy and security compliance. While our baseline standards may exceed compliance in some countries, we also recognize that our global approach may not always capture every local variation in the growing number of privacy and security requirements across the world. For that reason, to the extent that the legal requirements require higher standards than those generally described in our Policy, we comply with those higher standards.

DISCUSSION:

Personal Data may only be collected for specific, explicit, and legitimate purposes and may not be further processed contrary to those intended purposes. Processing for an incompatible purpose is generally only permissible with the consent of the individual about whom the data relates (i.e., the individual) or if permitted by the national law of the respective country within or from which Personal Data is transferred.

DATA ECONOMY
The collection and processing of Personal Data must be necessary for the intended purpose. If it is possible to remove or partially remove identifiers, removal should be considered when feasible assuming that the cost of doing so is reasonable in light of the protections offered and risk to the individuals.

DATA QUALITY
The Personal Data must be factually correct and, as necessary, up-to-date. Appropriate and reasonable measures should be undertaken to correct, update, or delete incorrect, outdated, or incomplete data.

DATA SECURITY
The Company has implemented appropriate physical, technical, and organizational measures that are designed to protect the Personal Data that it collects and processes from loss, misuse, and unauthorized alteration, destruction, access, or acquisition. These measures are further described in the Company's security policies and procedures.

CONFIDENTIALITY
Only Authorized Workers, who have undertaken to observe data privacy and security requirements, are allowed to be involved in the processing of the Company's Personal Data. Those individuals are prohibited from using Personal Data for their own private purposes or making it accessible to any unauthorized person or entity. Unauthorized persons in this context includes individuals who do not require access to such data to perform their employment, or independent contractor, duties for the Company. The confidentiality obligation survives termination of employment or the contractor relationship.

SPECIAL CATEGORIES OF PERSONAL DATA
The Company takes steps to limit the collection and processing of Sensitive Personal Data to that which is necessary for its legitimate business purposes. In general, the Company only collects Sensitive Personal Data where it is legally required to do so, with the consent of the individual, or for some other lawful reason, such as in the case of a medical emergency, and applies protections to that data that are aligned with its sensitivity.

SHARING PERSONAL DATA
Third parties who are selected as contractors, suppliers or service providers for the Company must provide sufficient written guarantees that they will uphold a similar level of protection for Personal Data as that applied by the Company and otherwise respect the protection of personal rights of the individual.

TRANSFER OF PERSONAL DATA
The Company is a global organization. As such, we sometimes transfer Personal Data to affiliates in countries other than the country in which it was collected, and/or store Personal Data in databases that are accessible in other countries. While some of those countries may not provide the same levels of privacy and security protection as the country from which the data originated, the Company has taken steps to ensure that the Personal Data is protected by entering into a data transfer agreement with its affiliates in other countries, which is consistent with the European Commission's Standard Contractual Clauses or other approved data transfer agreement. The Company also requires third parties to which we grant access to our data provide assurances that they apply equivalent standards to those contained in this Policy and that applicable data transfer laws that may apply to such transfers are followed.

RIGHTS OF INDIVIDUALS
In accordance with legal requirements and subject to any relevant exceptions, the Company upholds the rights of individuals to access Personal Data held about them, and to request correction or deletion of their data. The individual may address any such request to the local Company Human Resources Department of the respective country where the data was provided. There are some limitations on these rights, and if the request by the individual for correction or deletion is rejected, the individual will be informed about the reason for such rejection.

QUESTIONS AND COMPLAINTS/REMEDIES
Individuals may contact the Legal Department at FHOUKBR-Privacy@kbr.com at any time with any questions or complaints regarding the processing of Personal Data. Such questions and complaints will be treated confidentially and there will be no retaliation for complaints made in good faith by individuals.

If the issue raised by an individual is not remedied, the individual may file a complaint with the Company. The Company has put in place an internal process to evaluate privacy and security complaints and, in accordance with the legal obligations that apply, will investigate the complaint and respond to the individual. If the individual is not satisfied with the outcome of the complaint, he/she may request an additional escalated review within KBR. An individual may also, at any time and without permission from or notice to KBR, file a complaint with the relevant regulatory authority for data privacy in the location where the alleged data mismanagement took place.

DATA RETENTION
The Company retains personal data in accordance with its data retention schedules and legal and contractual requirements and takes steps to ensure secure destruction of the data.

IMPLEMENTATION AND ENFORCEMENT
The Company must ensure compliance with the principles embodied in this Policy. In that respect, Company managerial employees are required to ensure that this Policy is implemented. This includes in particular providing information about this Policy to Company employees and taking steps to ensure that this Policy is followed. They shall also take steps to ensure that any violations are addressed in a manner commensurate with the situation.

OBLIGATION TOWARDS DATA PROTECTION AGENCIES
The Company cooperates with the data protection agencies that are responsible for privacy and security compliance in the countries where the Company operates.

ROLES AND RESPONSIBILITIES:

ACCOUNTABILITY FOR OUR ACTIONS
The Company maintains programs to monitor periodically our adherence to this Policy and to help ensure compliance with this Policy, as well as with applicable laws or contractual agreements on the handling of Personal Data.

AMENDMENT OF THE POLICY AND CONTINUED APPLICATION
The Company reserves the right to amend this Policy as necessary, for instance to comply with changes to statutes, regulations, requirements of data protection agencies or internal procedures.

Should this Policy become invalid, irrespective of the reasons or causes for such invalidity, the Company will take steps to correct the invalidity and issue an updated Policy that shall apply prospectively to the Personal Data collected.

DEFINITIONS:

"Authorized Workers" means Company employees, contractors, supplied workers, and other third parties who are authorized to access Personal Data in connection with their employment, or their contractual duties, and who are obligated by agreement or Company policy or procedures to maintain the confidentiality of Personal Data.

"Company" means KBR, Inc., a Delaware corporation, its Business Units, subsidiaries, affiliates, and successors.

"Personal Data" refers to any data that directly or indirectly can lead to the identification of a living person, such as their name, address, e-mail address, telephone number, Social Security or other national identification number, employee identification number, driver's license number, medical identification number, photograph, or other identifying characteristic.

"Sensitive Personal Data" refers to the following categories of information: (a) race/ethnicity, (b) health information, (c) sexual orientation, (d) criminal history information, (e) trade union membership, (f) biometric data, (g) genetic data, (h) religion or philosophical beliefs, (i) political affiliation, and (j) compensation.

REFERENCES:

PR-GL-KBR-LL-1019 EU – U.S. Privacy Shield Procedure
PR-GL-KBR-IT-0811 IT Major Security Incident Response Procedure
PR-GL-KBR-IT-0815 Security Access and User Account Management Procedure
PR-GL-KBR-IT-0813 IT Global Password Standard Procedure
P-GL-KBR-IT-0801 Information Technology – Security and Acceptable Use Policy

---

APPROVED BY: CEO **DATE:** October 11, 2021

SUPERSEDES: P-GL-KBR-LL-1012, dated May 28, 2019