CRITIGEN

CRITIGEN LLC

EU EMPLOYMENT DATA PROTECTION STANDARDS

I. OBJECTIVE

The aim of these Employment Data Protection Standards ("Standards") is to provide adequate and consistent safeguards for the handling of Employment Data by Critigen U.K. Limited (Information Commissioner's Office Registration Number: Z3335338) in accordance with the regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), which is directly applicable since 25 May 2018 in all EU Member States and any implementing national legislation.

Critigen complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Critigen has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall prevail and apply on the US territory only. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

II. SCOPE

These standards apply to all Critigen entities within the EU that process Employment Data.

Processing is defined as any action that is performed on Employment Data, whether in whole or in part by automated means, such as collecting, modifying, using, disclosing or deleting such data.

Employment Data are defined as any information about an identified or identifiable person that is obtained in the context of a person's working relationship with Critigen. Such persons include, for example, job applicants, employees (whether temporary or permanent), contingent workers, retirees, and former employees, as well any dependents whose personal data have been given to Critigen by such persons.

These standards do not cover data rendered anonymous or where pseudonyms are used. Data are rendered anonymous if individuals are no longer identifiable or are identifiable only with disproportionately large expense in time, cost or labor. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either impossible or at least rendered considerably more difficult. If data rendered anonymous become no longer anonymous (i.e. individuals are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then these Standards shall apply again.

CRITIGEN

APPLICATION OF LOCAL LAWS

These Standards are designed to provide compliance with all applicable laws and in particular the GDPR and national implementing legislation. Critigen recognizes that certain laws might be modified to require stricter standards than those described in these Standards, in which case the stricter standards shall apply. Critigen will handle Employment Data in accordance with local law at the place where the Employment Data are processed. If applicable law provides for a lower level of protection of Employment Data than that established by these Standards, then these Standards shall apply. Any questions about applicable legislation and Critigen's compliance with it shall be addressed to Critigen's HR department in London or the Human Resources department at Critigen's headquarters. (for contact details, see Section XIV).

III. PRINCIPLES FOR PROCESSING EMPLOYMENT DATA

Critigen respects employee privacy and is committed to protecting Employment Data in compliance with all applicable laws and regulations. This compliance is consistent with Critigen's desire to keep its employees informed and to recognize and respect their privacy rights. Critigen will observe the following principles when processing Employment Data:

- Data will be processed fairly and in accordance with applicable laws.
- Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes.
- Data will be relevant to and not excessive for the purposes for which they are collected and used. For example, data may be rendered anonymous if deemed reasonable, feasible and appropriate, depending on the nature of the data and the risks associated with the intended uses.
- Data will be accurate and, where necessary kept up up-to-date. Reasonable steps will be taken to rectify or delete Employment Data that is inaccurate or incomplete.
- Data will be kept only as it is necessary for the purposes for which it was collected and processed. Those purposes shall be described in these Standards.
- Data will be processed in accordance with the individual's legal rights (as described in these Standards or as provided by law).
- Appropriate technical, physical and organizational measures will be taken to prevent unauthorized access, unlawful processing and unauthorized or accidental loss, destruction or damage to data. In case of any such violation with respect to Employment Data, Critigen will take all necessary steps to end the violation and determine liabilities in accordance with applicable law.

Critigen shall ensure that the same principles are observed by any third entity with which Critigen has entered a transaction if that entity collects and/or processes employment data in accordance with Section VIII of these Standards.

V. TYPES OF DATA PROCESSED

As permitted by local laws, the personal information we collect may include, but is not limited to,your:

- Name
- Home Address and Telephone Number
- Date of Birth
- Gender
- Ethnicity
- Language Skills
- Marital Status
- Emergency Contact Information
- Dependent Identification
- Education Level
- Training Levels
- Salary/Payroll (i.e. bank account, tax codes, P11D's)
- Hours of Employment
- Vacation and other Leave Time
- Insurance Information
- Benefits and Retirement Plan
- Performance Information
- Membership in Professional or Trade Associations
- Travel Preferences
- Recruitment information and Curriculum Vitae or Resume
- Other information you have provided us

Critigen does not collect or process sensitive data **(**such as data revealing political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures). Critigen only collects data on ethnic origin for the purposes of demonstrating that we are an equal opportunities employer. Critigen shall ensure that no sensitive data is collected and/or processed by a third entity with which Critigen has entered a transaction in accordance with Section VIII of these Standards. In the unlike event that such a collection or processing is required for the legitimate purposes described under chapter VII, Critigen will ensure that the individual is informed of such collection or processing in order to provide his or her explicit consent for such collection or processing.

CRITIGEN

VI. WAYS OF OBTAINING EMPLOYMENT DATA

The ways by which Critigen obtains Employment Data are defined hereby. Critigen does not obtain any personal information about employees unless the employee has provided that information to Critigen by completion of a written employment application, employee benefits application, insurance form, consent form, survey, or completion of an on-line or hard copy form. Employees may choose to submit personal, private information by facsimile, regular mail, e-mail or electronic transmission over our internal web site, interoffice mail, or personal delivery.

VII.PURPOSES FOR EMPLOYMENT DATA PROCESSING

Critigen processes personal data for legitimate purposes related to human resources, business and safety /security. The limitation of purposes shall be taken into consideration before any type of processing of Employment Data and shall not be subject to any changes without prior notification. These principal purposes include:

- **Human Resources and Personnel Management:** Human resource processes are activities to maintain a workforce for Critigen. Examples include recruiting, on boarding, payroll processing, invoice processing, administration of employee benefits, internal resource management, complying with applicable legal requirements and communicating with employees and/or other representatives.
- **Business Process Execution and Management**: Business processes are activities to run the operation of Critigen. Examples include scheduling, managing company assets, populating employee directories and general business development. Personal data may be sent to brokers, vendors, and potentially clients as needed to conduct business.
- **Safety and Security**: Safety/security processes are activities to ensure the safety and protection of Critigen's workers, resources and communities. Examples include protecting occupational health and safety and authenticating worker status to authorize access to Critigen resources and facilities.

If the employee fails to provide certain information when requested, Critigen will not be able to fully per-form the contract, or could be prevented from complying with its legal obligations.

If Critigen introduces a new process or application that will result in the processing of Employment Data for purposes that go beyond the purposes described above, Critigen will ensure that the concerned employees are informed of the new process or application, the purpose for which the employment data are to be used and the categories of recipients of the Employment Data. Critigen shall ensure that the processing of Employment Data by third party entities with which Critigen has entered a transaction is conducted only for the same or similar purposes as the ones described under the present Section of these Standards.

VIII. DATA CONTROL AND/OR PROCESSING BY THIRD ENTITIES

Critigen may from time to time enter into transactions with third entities, the consummation of which may require the joint control and or processing of your personal data with such third entities.

Critigen shall ensure that third entities, with which transactions are entered that may require transfer of employees and their data to such entities and subsequently control and processing of such data by these entities, are registered with the Information Commissioner's Office in the UK or any other competent Data Protection Authority in the EU and comply with adequate data protection standards in application of the GDPR and any national implementing legislation.

Critigen shall ensure that third entities, with which transactions are entered that may require transfer of employees and their data to such entities and subsequently control and processing of such data by these entities, apply adequate security safeguards in the control and processing of your personal data, which result in a level of protection equal or higher to that ensured by Critigen as described in detail in Section IX of these Standards.

IX. SECURITY AND CONFIDENTIALITY

Critigen is committed to taking appropriate technical, physical and organizational measures to protect Employment Data against unauthorized access, unlawful processing, accidental loss or damage and unauthorized destruction.

Equipment and Information Security

To safeguard against unauthorized access to Employment Data by third parties outside Critigen, all electronic Employment Data held by Critigen are maintained on Systems that are protected by up-to-date secure network architectures that contain firewalls and intrusion detection devices.

Access security

The importance of security for all personally identifiable information associated with Critigen's employees is of highest concern. Critigen is committed to safeguarding the integrity of personal information and preventing unauthorized access to information maintained in Critigen's database. These measures are designed and intended to prevent corruption of data, block unknown and unauthorized access to our computerized system and information, and to provide reasonable protection of Employment Data in Critigen's possession. All employee files are confidentially maintained in the HR department in secured and locked file cabinets or rooms. Access to the computerized database is controlled by a log-in sequence and requires users to identify themselves and provide a password before access is granted. Users are limited to data required to perform their job function. Security features of our software and developed processes are used to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

CRITIGEN

Training

Critigen will be responsible for conducting training regarding the lawful, enumerated intended purposes of processing Employment Data, the need to protect and keep information accurate and up-to-date, and the need to maintain the confidentiality of the data to which employees have access. Authorized users will comply with these Standards and Critigen will take appropriate actions in accordance with applicable law, if Employment Data are accessed, processed, or used in any way that is inconsistent with the requirements of these Standards.

Critigen shall ensure that similar confidentiality and security measures are applied by any third entities with which transactions are entered that may require transfer of employees and their data to such entities and subsequently control and processing of such data by these entities. These measures shall ensure a level of protection equal or higher to that afforded by Critigen and described in these Standards.

X. RIGHTS OF DATA SUBJECTS

Any person has the right to be provided with information as to the nature of the Employment Data stored or processed about him or her by Critigen. All employees have access to their own personal information and may correct or amend it as needed. Employees may view their own personnel record upon request by contacting the local HR contact or by accessing certain information in PeopleSoft employee self-service**.**

If any information is inaccurate or incomplete, the person may request that the data be amended. It is every person's responsibility to provide HR with accurate employment Data about him or her and to inform HR of any changes. (e.g. new home address or change of name).

If the person demonstrates that the purpose for which the data is being processed in no longer legal or appropriate, the data will be deleted, unless the law requires otherwise.

Please note that if an employee stores their own personal information on company provided equipment, that they do so at their own risk. The company will use the automatic back up software to maintain systems and data integrity, but cannot be held responsible for data that it is not aware of nor does it process. If Critigen finds non-business related personal information on company provided equipment, it will not be used.

CRITIGEN

XI. TRANSFERS

In connection with the activities described under Chapter VII, Critigen transmits Employment Data outside of the employees' country to the computer database located at Critigen's corporate headquarters in United States of America. Moreover, Employment Data is transmitted to third parties via secure website or portal and is maintained in U.S. secure data centers.

- **Selected Third Parties:** Critigen will not disclose or share any employee's personal information with any external entity or third party, except to an employee's designated insurance provider, employee benefits administrator, payroll provider, travel professionals, clients to illustrate experience and qualifications for business purposes or promotion and not beyond that, and/or to a third entity with which Critigen has entered a transaction as described under section VIII of these Standards or as an employee designates.

- **Other Third Parties:** Critigen may be required to disclose certain Employment Data to other third parties: (1) As a matter of law (e.g. to tax and social security authorities); (2) to protect Critigen's legal rights; or (3) in an emergency where the health or security of an employee is endangered (e.g. a fire).

XII. DIRECT MARKETING

Critigen will not disclose Employment Data to entities outside Critigen or use non-work contact data (e.g. home address or telephone number) to offer any products or services to Critigen employees for personal or familial consumption ("direct marketing") without his or her prior consent. Further, Critigen will not use workplace contact data (e.g. work address or e-mail address) to conduct direct marketing unless recipients are given an opportunity to opt out of receiving any direct marketing communications.

The restrictions in this section apply to contact data obtained in the context of a working relationship with Critigen. They do not apply to contact data obtained in the context of a consumer or customer relationship. Critigen retains the right to communicate information to Critigen's employees about employee benefits or about Critigen supported charitable programs.

CRITIGEN

XIII. AUTOMATED DECISIONS

Automated decisions are defined as decisions about individuals that are based solely on the automated processing of data and that produce legal effects that significantly affect the individuals involved.

Critigen does not make Automated Decisions for employees' evaluation. If Automated Decisions are made, affected persons will be given an opportunity to express their views on the Automated Decision in question and object to it.

XIV. ENFORCEMENT RIGHTS AND MECHANISMS

Critigen will ensure that these Standards are observed. All persons who have access to Employment Data must comply with the Standards. If at any time, a person believes that Employment Data relating to him or her has been processed in violation of these Standards, he or she may report the concern to the competent Critigen official. In compliance with the Privacy Shield Principles, Critigen commits to resolve complaints about our collection or use of employee's personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Sarah Ford, UK Human Resources Administrator or Jeanine Willis, Corporate office Director Human Resources at:

Local Office:
Ms. Sarah Ford
Critigen U.K. Limited
Spaces Covent Garden
60 St. Martin's Lane
London
WC2N 4JS
44(0) 207 8126683
sarah.ford@critigen.com

Corporate Office:
Ms. Jeanine Willis
Critigen LLC
1430 Summit Ave, Suite 100C
Seattle WA 98122
USA
1+(206) 321-4200
1+(206) 602-8888 Fax
jeanine.willis@critigen.com

If your concerns cannot be resolved by working with a member of Human Resources, your concerns will be reviewed by a member of the Critigen executive leadership team for resolution. Critigen commits to reviewing and responding to a complaint made by an employee within 45 days of receipt of the complaint.

Critigen has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the UK business entity to the US business entity, in the context of the employment relationship.

Furthermore, Critigen is subject to:

- the investigatory and enforcement powers of the Federal Trade Commission (FTC)
- the possibility, under certain conditions, for the individual to invoke binding arbitration
- the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements
- liability in cases of onward transfers to third parties

To learn more about Privacy Shield, understand your rights, or to file a complaint, please visit https://www.privacyshield.gov/

XV. AUDIT PROCEDURES

Critigen uses role based security in its infrastructure, in which rights are based on necessity to perform daily job function. For instance, only staff that require access to employee personal data will have permissions. Critigen performs and audit review of its change controls every 90 days. Terminated employees are removed from the systems and security access will be terminated in accordance with company security standards.

XVI. COMMUNICATION ABOUT THE STANDARDS

In addition to the training on these standards, Critigen will communicate these standards to current and new employees by posting them on Critigen's internal SharePoint website**.** **https://critigenllc.sharepoint.com/Office/SitePages/Home.aspx**

XVII. MODIFICATIONS OF THE STANDARDS

Critigen reserves the right to modify these Standards as needed, for example, to comply with changes in laws, regulations or requirements imposed by data protection authorities or to adopt to circumstances created by a corporate transaction involving the company and/or any other factual

circumstances**.** Changes must be approved to the designated Critigen's Chief Privacy leader or his/her designee for the amended Standards to enter into force. If Critigen makes changes to the Standards, these Standards will be submitted for renewed approval according to the relevant applicable provisions of the law. Critigen will inform Critigen employees and other persons (e.g. persons accessing Critigen websites to enter Employment Data such as job application information) of any material changes in the Standards. Critigen will post all changes to the Standards on relevant internal and external websites.

Effective with the implementation of these Standards, all existing intra-group agreements and applicable company privacy guidelines relating to the processing of Employment Data will be superseded by the terms of these Standards. No other internal policy shall be applicable with respect to the Protection of Employment Data handled by Critigen. All parties to such agreements will be notified of the effective date of the implementation of the Standards.

XVIII. OBLIGATIONS TOWARDS DATA PROTECTION AUTHORITIES

Critigen will respond diligently and appropriately to requests from data protection authorities about these Standards or compliance with applicable data protection privacy laws and regulations. Critigen's employees who receive such requests should contact their human resources manager or business legal counsel. Critigen will, upon request, provide data protection authorities with names and contact details of relevant persons. With regard to transfers of Employment Data between Critigen entities, the importing and exporting Critigen entities will (i) cooperate with inquiries from the data protection authority responsible for the entity exporting the data and (ii) respect its decisions, consistent with applicable law and due process rights. With regard to transfers of data to third entities, Critigen will comply will cooperate with all competent data protection authorities in accordance with applicable legislation.

ADDENDUM

Rights and obligations with Respect to Employment Data Collected Within the EU/EEA and

Processed Elsewhere.

In addition to any rights and obligations that are set forth in Critigen's EU Employment Data Protection Standards ("Standards") or that otherwise exist, the following principles established in light of the GDPR and national implementing legislation shall apply to Employment Data collected by Critigen in the EU/EEA and processed elsewhere. The enforcement rights and mechanisms mentioned in the Standards also apply to the

provisions of this Addendum. The following are not intended to grant employees further rights or establish further obligations beyond those already provided under the GDPR and national implementing legislation.

1. Employees may object to the processing of Employment Data about them on compelling legitimate grounds relating to their particular situation. This might occur, for instance, if the employer's life or health is at risk due to the processing of the data. This provision shall not apply if the processing is (i) required by law; (ii) based on the employee's individual consent or (iii) necessary to fulfill a contractual obligation between the employee and Critigen; (iv) required for the completion of a transaction as described under Section VIII of these Standards.

2. After exhausting appropriate internal dispute resolution processes, employees may seek compensatory damages from Critigen for loss or damage to them caused by a violation of the Standards (including the provisions of this Addendum) by Critigen. Critigen shall not be liable for damages if it has observed the standard of care appropriate in the circumstances.

3. If any of the terms or definitions used in the Standards are ambiguous, the definitions established under applicable local law within the relevant EU/EEA Member State shall apply or where there are no such definitions, the definitions of the GDPR shall apply

Collection and Management of Data

Any data placed on Critigen equipment (laptop, desktop, mobile device, server, SAN/NAS, etc.) is subject to being backed up for business continuity. Any of these locations or devices will have consistent security and backup that meets or exceeds company standards. The employee is made aware that any data stored or transmitted via Critigen's equipment is subject to the backup process and will be accessible by staff that should have access to conduct their job.

Critigen uses role based security in its infrastructure, in which rights are based on necessity to perform daily job function. For example, only staff that should have access to employee personal data will be granted permissions of access. Critigen performs an audit review of its change controls every 90 days.

NOTICE: These Standards do not negate other company policies that employees must adhere to (i.e. IT Employee Acceptable Use policy, Wireless Mobility policy, Information Security policy etcetera.