Fluor UK Data Protection Binding Corporate Rules Policy

PART I: INTRODUCTION AND BACKGROUND

Purpose

This Data Protection Binding Corporate Rules Policy ("Policy") establishes the approach of Fluor to compliance with UK data protection law and specifically to transfers of personal data from the Fluor entities in the UK to the Fluor entities outside the UK.

Scope

This Policy applies to all Fluor entities and their employees and contains 16 rules ("Rules"). Fluor entities and their respective employees must comply with and respect this Policy when processing personal data of Fluor employees, and those of their clients, business or contracting partners, suppliers or other third parties. This Policy does not replace any specific data protection requirements that might apply to a specific business area or function but where any such requirements do not meet the standards set out by the Rules in this Policy, Fluor will in any event process personal data subject to the Policy adhering to the Rules in this Policy.

Transfers of personal data take place between the Fluor entities during the normal course of business and such data may be stored in centralised databases accessible by Fluor entities from anywhere in the world.

For the purposes of this Policy:

"GDPR" means the European Union (EU) Regulation 2016/679 (the General Data Protection Regulation).

"ICO" means the Information Commissioner’s Office.

"Personal data" means information that is subject to UK data protection law relating to an identified or identifiable natural person ("data subject"); an identifiable natural person 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 natural person.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"UK" means the United Kingdom.

“UK data protection law" means the United Kingdom’s Data Protection Act 2018, the UK GDPR and regulations made thereunder as amended from time to time.

"UK GDPR" means the GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and 2020 and its successor laws.

The terms “controller”, “processor” and "data subject" have the meanings given to them in the GDPR.

Policy Access

This Policy is published on the Fluor intranet accessible on OneFluor's Career & Life Resources page within the HR Toolkit, Policies, and on the Fluor website accessible at https://www.fluor.com/SiteCollectionDocuments/fluor-data-protection-policy.pdf.

BACKGROUND

WHAT IS DATA PROTECTION LAW?

Data protection law gives people the right to control how their personal data is processed, and establishes restrictions on how such information may be processed. When Fluor processes the personal data of its employees, or that of its clients, business or contracting partners, suppliers or other third parties, this processing is covered and regulated by data protection law.

HOW DOES DATA PROTECTION LAW AFFECT FLUOR INTERNATIONALLY?

Data protection law in a particular jurisdiction can impact how Fluor and its employees can handle such information worldwide. For example, UK data protection law does not allow the transfer of personal data to countries that do not ensure an adequate level of data protection without certain protections being put into place, and without compliance with certain procedures. Many of the countries in which Fluor operates are not regarded by UK data protection law as providing an adequate level of protection for data subjects' data privacy rights, and therefore Fluor must take steps to assure that that data is adequately safeguarded.

WHAT IS FLUOR DOING ABOUT IT?

Fluor has created this Policy together with the appendices referenced herein in order to assure that personal data in its possession is handled securely, and that its privacy is maintained. This Policy and the appendices also ensure that personal data is processed consistently in all jurisdictions in which Fluor operates. The purpose of this Policy is to set out a general framework to satisfy the standards contained in UK data protection law so as to provide an adequate level of protection for all personal data transferred from the Fluor entities within the UK to Fluor entities outside the UK.

Central to this Policy are 16 Rules based on, and interpreted in accordance with, relevant UK data protection standards that must be followed. All Fluor entities and employees are legally bound to comply with this Policy.

WHAT DOES THIS MEAN IN PRACTICE FOR PERSONAL DATA PROCESSED?

Employees of Fluor and of its clients, business or contracting partners, suppliers or other third parties whose personal data is processed in the UK, and is then transferred to Fluor entities outside the UK, benefit from certain additional rights to enforce the Rules set out in this Policy. These data subjects have the right to seek to enforce compliance with Rules 1B, 1C, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14 and 16 of this Policy, as well as these liability and jurisdiction provisions and Fluor's commitment to provide easy access to this Policy by:

- lodging a complaint with the ICO;
- bringing a claim before the UK courts against the Fluor UK entity that is responsible for exporting the personal data ("Exporting Fluor UK Entity");
- complaining to the Exporting Fluor UK Entity, seeking appropriate redress from the Exporting Fluor UK Entity, (which agrees to take the necessary action to remedy any breach of the Policy by any Fluor entity outside the UK that processes personal data

received from that Exporting Fluor UK Entity) and, where appropriate, receiving compensation from the Exporting Fluor UK Entity for any damage suffered as a result of a breach of this Policy by Fluor in accordance with the determination of a court or other competent authorities; and/or

- obtaining a copy of this Policy and the binding mechanism entered into by Fluor in connection with this Policy.

In the event of a claim being made in which a data subject has suffered material or non-material damage where that data subject can demonstrate that it is likely that the damage has occurred because of a breach of the Policy, Fluor has agreed that the burden of proof to show that a Fluor entity outside the UK is not liable for the breach, or that no such breach took place, will rest with the Exporting Fluor UK Entity.

Fluor has appointed a Chief Privacy Officer as the person to oversee and ensure compliance with this Policy. The Chief Privacy Officer reports directly to the Head of Compliance, who in turn reports to Fluor's Chief Legal Officer who reports to Fluor's Chief Executive Officer. The Chief Privacy Officer's role includes informing and advising the highest management on risks (for example, by providing quarterly updates on new privacy and cybersecurity risks), dealing with ICO's investigations, and monitoring reports on compliance at a global level. The Chief Privacy Officer works in active cooperation with Legal, Human Resources, Compliance, Information Technology, Audit, other required or appropriate departments and/or data privacy officers or leads at the regional and country level who are responsible for overseeing and enabling compliance with this Policy on a day-to-day basis. Employees responsible for dealing with privacy issues at a local level are in charge of handling local complaints from data subjects, reporting major privacy issues to the Chief Privacy Officer, and monitoring training and compliance at a local level.

WHAT DATA TRANSFERS ARE COVERED BY THIS POLICY?

The personal data processed by Fluor is typical of a large business organization.

In relation to **employees**, the personal data includes name; work and personal contact information; employment information including recruitment information, role, salary, bank account information, dependants, benefits, appraisals, training, disciplinary and grievance procedures, images, sickness absence and safety incident reports; IT access information; CCTV recordings; and equalities reporting (ethnicity data).

In relation to **clients**, the personal data may include name; contact information; details of goods and services provided; and CCTV recordings.

In relation to **business or contracting partners, suppliers or other third parties**, the personal data may include name; contact information; details of goods and services provided; CCTV recordings; access control information; images; background check information; training records; and security vetting information.

This Policy covers transfers of the abovementioned personal data:

- between the UK and Fluor's main offices and Fluor project offices located in the Netherlands, Spain, Poland and Ireland for the purpose of employee administration;
- from the UK to the United States, for the purpose of HR administration for Fluor;
- corporate financial administration and public company reporting on behalf of Fluor;
- storage and archiving; and
- from both the United States, and the UK, outward to individual project offices or project sites all over the world, for the purposes of local payroll administration at the project level, and to execute HR functions locally over both local hires and existing Fluor employees sent to project sites on international assignment.

CONTACT AND OTHER INFORMATION

Fluor Corporation, as the holding company parent of its operating subsidiaries that are bound by this Policy, may be contacted through its representatives listed below. Further contact details for Fluor Corporation, and its local company offices and other locations, including all locations that are bound by this Policy (as well as some locations which are not bound by the Policy) may be found through its website, www.fluor.com/about-fluor/locations and for TRS entities, through its website, at https://www.trsstaffing.com/contact-us.

If you have any questions about which Fluor entities are bound by the Policy, or you require a list of entities bound by the Policy you may contact Fluor's Chief Privacy Officer or Fluor's Chief Compliance Officer at the addresses below. If you have any other question that relates to the processing of your personal data at a particular Fluor location, or if you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues you may also contact Fluor's Chief Privacy Officer or Fluor's Chief Compliance Officer at the addresses below, who will either deal with the matter or forward it to the appropriate person or department within Fluor.

Chief Privacy Officer chief.privacy.officer@fluor.com 6700 Las Colinas Blvd. Irving, TX 75039 USA
Chief Compliance Officer corporate.compliance@fluor.com 6700 Las Colinas Blvd. Irving, TX 75039 USA

The Chief Privacy Officer is responsible for ensuring that changes to this Policy are notified to the Fluor entities and to data subjects whose personal data is processed by Fluor.

If you are concerned about the way in which Fluor has processed your personal data, you may follow the Complaint Handling Procedure which is set out in Appendix 3.

PART II: BINDING CORPORATE RULES

The Rules are divided into two sections. Section A addresses the basic principles of UK data protection law which Fluor must observe when Fluor processes personal data.

Section B deals with the practical commitments made by Fluor to the ICO in connection with this Policy.

SECTION A BASIC PRINCIPLES OF UK DATA PROTECTION LAW

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1A – Fluor will first and foremost comply with local law where it exists.

As an organization, Fluor will always comply with applicable legislation relating to personal data (for example, in the UK, the UK GDPR) and will ensure that where personal data is processed in the UK this is done in accordance with UK data protection law.

Where there is no applicable local law or local law does not meet the standards set out by the Rules in this Policy, Fluor will in any event process personal data subject to the Policy adhering to the Rules in this Policy.

Where applicable data protection law requires a higher level of protection than is provided for in this Policy, the higher level of protection will take precedence.

Rule 1B - Fluor will ensure that its processing of personal data is fair and lawful and that a legal basis exists for the processing of personal data where required.

Fluor will ensure that its processing of personal data is fair and lawful, and that a legal basis for processing personal data exists where required. Taking into account any specific provisions of UK law, Fluor will only process personal data where:

- the data subject has given consent to the processing of his or her personal data and that consent meets the required standards under UK data protection law;
- it is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject before entering into a contract;
- it is necessary for compliance with a legal obligation to which Fluor is subject where that legal obligation derives from UK law;
- it is necessary in order to protect the vital interests of the data subject or of another data subject;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Fluor where that processing is set out under a UK law to which Fluor is subject; or

- it is necessary for the purposes of the legitimate interests pursued by Fluor or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Where the processing of personal data relates to criminal convictions and offences or related security measures, Fluor will not carry out such processing otherwise than under the control of official authority or when the processing is authorised by UK law that provides appropriate safeguards for the rights and freedoms of data subjects.

Rule 1C – Fluor will only process special category personal data where the data subject's explicit consent has been obtained unless Fluor has an alternative legal basis for doing so.

Processing of special category personal data (as defined at Rule 7) is only permitted on certain grounds, for example, where the:

- data subject has given explicit consent to the processing of any special category of personal data for one or more specified purposes, unless UK data protection law provides that the prohibition on processing special category data may not be lifted by a data subject;

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Fluor or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by UK law or a collective agreement pursuant to UK law providing for appropriate safeguards for the fundamental rights and interests of data subjects;

- processing is necessary in order to protect the vital interests of a data subject where that data subject is physically or legally incapable of giving consent;

- processing relates to personal data that is manifestly made public by the data subject;

- processing is necessary for the establishment, exercise or defence of legal claims;

- processing is necessary for reasons of substantial public interest on the basis of UK law provided that it is proportionate to the aim pursued, respects the essence of data protection and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

- processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of UK law, provided that the processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under UK law or by rules established by national competent bodies; or

- processing is necessary for reasons of public health which provides for suitable and specific measures to safeguard the rights and freedoms of data subjects, in particular duties of professional confidentiality.

Rule 1D – Fluor will assess the impact of any processing of personal data that will involve high risks to the rights and freedoms of data subjects.

Fluor will assess the necessity and proportionality of any new processing of personal data that involves high risks to the rights and freedoms of data subjects in accordance with its privacy impact assessment process, as amended and updated from time to time. In the event that the data protection impact assessment indicates that the processing will result in a high risk to data subjects, Fluor may be required to consult the ICO prior to beginning processing in the absence of measures taken to mitigate the risk.

RULE 2 – ENSURING TRANSPARENCY AND USING PERSONAL DATA FOR A KNOWN PURPOSE ONLY

Rule 2A – Fluor will explain to data subjects how their personal data will be processed at the time Fluor obtains it from these data subjects.

Fluor will ensure that data subjects are always told in a clear and comprehensive way (usually by means of a fair processing statement) about the following matters: (a) the identity and contact details of the controller, its representative, and its data protection officer (as applicable); (b) the purposes of the processing, (c) the legal basis for processing and where required, the legitimate interests pursued by Fluor in processing personal data; (d) the recipients or categories of recipients of the personal data and the source and categories of information received from third parties; (e) that Fluor intends to transfer personal data to a third country outside the UK either where there exists an adequacy decision under UK law or, where there is no such decision, subject to suitable safeguards which will be described in the fair processing statement or otherwise made available to data subjects; (f) the period for which their data will be stored, or if that is not possible, the criteria used to determine that period; (g) the existence of the right to request access to, and rectification of, or erasure of, or to object to the processing of their personal data, to restriction of the processing of their personal data, or to port their personal data to another controller where technically feasible; (h) where applicable, typically as regards special categories of (that is, sensitive) personal data, the right to withdraw consent to processing; (i) the right to lodge a complaint with the ICO; (j) whether providing personal data is a contractual or statutory requirement, and the consequences of not providing personal data in such circumstances; and (k) information about any personal data that is processed for automated decision-making, including profiling.

The requirements of the UK data protection law that apply to the personal data will determine whether any additional information has to be provided to data subjects and the timescale within which the required information must be provided.

Where Fluor has obtained a data subject's personal data from a source other than that data subject, Fluor will inform the data subject and indicate where the personal data came from, and whether it came from publically available sources, and such information shall be provided

within a reasonable period after obtaining the personal data but in any event within one month, having regard to the specific circumstances in which the personal data are processed. If the personal data are processed to communicate with the data subject, Fluor will provide this information to the data subject at the time of first communication, or if it is to be disclosed to a third party, no later than the time when the information is first disclosed.

Fluor will follow this Rule 2A unless there is a legitimate basis for not doing so (for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, taxation purposes, legal proceedings or where otherwise permitted by UK data protection law).

Rule 2B – Fluor will only process personal data for those purposes which are known to the data subject or which are within their expectations and are relevant to Fluor.

This rule means that Fluor will comply with any applicable legislation relating to the processing of personal data. This means that Fluor may only process personal data for specific, explicit and legitimate purposes and not process personal data in a way which is incompatible with those purposes.

Fluor will identify and make known the purposes for which personal data will be processed (including the secondary purposes and disclosures of the data) by way of a privacy notice as described in Rule 2A.

Rule 2C – Fluor will only change the purpose for which personal data is processed if Fluor has a legitimate basis for doing so, consistent with UK data protection law.

If Fluor processes personal data for a specific purpose (as communicated to the data subject via the relevant fair processing statement) and subsequently Fluor wishes to process personal data for a different or new purpose, it will not further process the information in a way incompatible with the purpose for which it was collected unless Fluor has a legitimate basis for doing so, consistent with UK data protection law, and the relevant data subjects are notified of the changes.

In certain cases, for example, where the processing is of special categories of personal data, the data subject's consent to the new purposes or disclosures may be necessary.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – Fluor will keep personal data accurate and up to date and take every reasonable step to ensure that personal data that are inaccurate are erased or rectified without delay.

The main way of ensuring that personal data is kept accurate and up to date is by actively encouraging data subjects to inform Fluor when their personal data changes.

Rule 3B – Fluor will only keep personal data for as long as is necessary for the purposes for which the personal data are processed.

Fluor will comply with all Fluor record retention policies that apply company-wide and, as applicable, to a particular office or function.

Rule 3C – Fluor will only process personal data which is adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data are processed.

Fluor will identify the minimum amount of personal data that is required in order properly to fulfil its purposes.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – Fluor will always process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental or unlawful destruction, loss, alteration and unauthorised disclosure of or access to personal data using appropriate technical or organisational measures (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons).

Fluor will comply with the requirements in applicable data security and personal private and financial data handling policies that apply company-wide and, as applicable, to a particular office or function, as revised and updated from time to time. This includes Fluor's IT Security Policies.

Rule 4B – Fluor will ensure that providers of services to Fluor also adopt appropriate and equivalent security measures.

UK data protection law expressly requires that where a provider of a service to any of the Fluor entities has access to a data subject's personal data (e.g. a payroll provider), strict contractual obligations evidenced in writing dealing with the security of that data are imposed to ensure that such service providers act only on Fluor's instructions when using that data and that they have in place appropriate technical and organizational security measures to safeguard personal data and otherwise meet the requirements of UK data protection law.

Rule 4C – Where Fluor entities process personal data on behalf of other Fluor entities those entities will adhere to Rule 4A and act only on the instructions of the Fluor entity on whose behalf the processing is carried out.

Where a service provider is a Fluor entity processing personal data on behalf of another Fluor entity, the Fluor service provider must:

- act only on the documented instructions of the Fluor entity on whose behalf the processing is carried out;
- ensure that it has in place proportionate technical and organizational security measures to safeguard the personal data. Such instructions may be provided by means of a completed Processing Schedule (as set out in Appendix 6); and
- comply with the obligations set out in Part 2 of the Processing Schedule, or as appropriate, a contract or legal act entered into between the parties in relation to such processing which is consistent with UK data protection law in so far as it relates to the engagement of a processor.

Rule 4D – Fluor will adhere to its data breach notification policy.

Fluor will adhere to its data breach notification policy (as revised and updated from time to time) which sets out the process which must be followed in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (a "Data Protection Breach").

In particular, in the event of a Data Protection Breach, Fluor will, without undue delay, notify:

- the Chief Privacy Officer; and
- the ICO, unless the Data Protection Breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Data subjects will be notified in cases where the Data Protection Breach is likely to result in a high risk to their rights and freedoms unless such notification is not required under applicable law.

The Chief Privacy Officer will document Data Protection Breaches suffered by Fluor, the effects of such incidents and the remedial action taken in a Data Protection Breach report which will be available to the ICO on request.

RULE 5 – HONORING DATA SUBJECTS' RIGHTS

Rule 5A – Fluor will adhere to the Data Subjects' Rights Request Procedure.

Data subjects are entitled (by making a request to Fluor) to be supplied with a copy of personal data held about them (including both electronic and paper records). Fluor will follow the steps set out in the Data Subjects' Rights Request Procedure (see Appendix 1) when dealing with requests from data subjects for access to their personal data.

Rule 5B – Fluor will deal with requests to rectify, erase, restrict, or port personal data or objections to the processing of personal data in accordance with the Data Subjects' Rights Request Procedure.

Data subjects are entitled to request rectification, erasure, or restriction, as appropriate of their personal data; exercise their right to portability in relation to their personal data; and/or object to the processing of their personal data, including processing for direct marketing purposes and to profiling to the extent that it is related to such marketing. Fluor will follow the steps set out in the Data Subjects' Rights Request Procedure (see Appendix 1) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR OVERSEAS TRANSFERS

Rule 6 – Fluor will not transfer personal data to third parties outside Fluor without ensuring adequate protection for the data in accordance with the standards set out by this Policy and in accordance with UK data protection law.

In principle, transfers of personal data outside Fluor from the UK to a country or an international organisation that has not been found to offer an adequate level of protection for personal data under UK data protection law are not allowed without appropriate steps being taken, in accordance with UK data protection law, such as:

- signing up to Model or contractual clauses;
- confirming that the third party offers safeguards (which the UK Secretary of State has found to offer an adequate level of protection for the UK personal data transferred); or
- ensuring that the transfer is necessary for: (a) the performance of a contract between the data subject and Fluor or for the implementation of pre-contractual measures taken at the data subject's request; (b) the conclusion or performance of a contract concluded in the interest of the data subject between Fluor and another party; (c) important reasons of public interest; (d) the establishment, exercise or defence of legal claims; (e) the protection of the vital interests of the data subject or of another data subject and where the data subject is incapable of giving consent; or f) obtaining the explicit consent of the data subject having informed the data subject of the risks of the transfer.

RULE 7 – SAFEGUARDING THE PROCESSING OF SPECIAL CATEGORY DATA

Rule 7 – Fluor will only process special category personal data if it is absolutely necessary to process it.

Special categories of personal data (also referred to as 'sensitive personal data') is data relating to a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sex life or sexual orientation, genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health. Fluor will assess

whether sensitive personal data is required for the proposed purpose and when it is absolutely necessary in the context of the business.

RULE 8 – LEGITIMIZING DIRECT MARKETING

Rule 8 – Fluor will allow clients, business or contracting partners, suppliers or other third parties to opt out of receiving marketing information.

All data subjects have the data protection right to object to the processing of their personal data for direct marketing purposes. This includes the right to object to profiling to the extent that it is related to such marketing. Fluor will honor all such opt out requests.

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 – Fluor will respect the right of data subjects not to be subject to a decision made as a result of the processing of personal data by automated means (including profiling) which has a legal or similarly significant effect on them, unless the processing is permitted under UK data protection law and Fluor has put in place necessary measures to protect the legitimate interests of data subjects.

Under UK data protection law no evaluation of or decision about data subjects which significantly affects them can be based solely on the automated processing of personal data unless:

- the processing is authorised under UK data protection law;
- the decision is necessary for entering into a contract between the data subject and Fluor; or
- the data subject has given their explicit consent.

and in such cases Fluor will put in place measures to protect the rights and freedoms and legitimate interests of data subjects, such as the right for a data subject to obtain human intervention in the decision, to express his or her point of view and to contest the decision.

SECTION B PRACTICAL COMMITMENTS MADY BY FLUOR

RULE 10 – ACCOUNTABILITY

Rule 10A – Fluor will implement appropriate technical and organisational measures to enable and facilitate compliance with this Policy in practice.

Taking into account the state of the art and cost of implementation, and the scope, nature, context and purposes of the processing, Fluor will implement appropriate technical and organizational measures which meet the principles of data protection by design and by default as required by UK data protection law.

Rule 10B – Fluor will maintain a written record of its processing activities and make that record available to the ICO on request.

The data processing records maintained by Fluor entities will contain:

- the Fluor entity's name and contact details;
- the purposes for which the personal data are processed;
- a description of the categories of data subjects about whom the personal data are processed and the personal data processed;
- the categories of recipients to whom personal data has been or will be disclosed;
- details of the third country or countries to which the personal data are transferred;
- where possible, the period for which the personal data will be retained; and
- where possible, a general description of the technical and organisational security measures used to protect the personal data.

RULE 11 – TRAINING

Rule 11 – Fluor will provide appropriate training to employees who have permanent or regular access to personal data, who are involved in the processing of personal data or in the development of tools used to process personal data.

RULE 12 – AUDIT

Rule 12 – Fluor will comply with the Binding Corporate Rules Policy Audit Protocol set out in Appendix 2.

RULE 13 – COMPLAINT HANDLING

Rule 13 – Fluor will comply with the Binding Corporate Rules Policy Complaint Handling Procedure set out in Appendix 3.

RULE 14 – COOPERATION WITH THE ICO

Rule 14 – Fluor will comply with the Binding Corporate Rules Policy Co-operation Procedure set out in Appendix 4.

RULE 15 – UPDATE OF THE RULES

Rule 15 – Fluor will comply with the Binding Corporate Rules Policy Updating Procedure set out in Appendix 5.

RULE 16 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 16A – Fluor will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on the guarantees provided by the Policy, Fluor will promptly inform the Chief Privacy Officer unless otherwise prohibited by law or by a law enforcement authority.

Rule 16B – Fluor will ensure that where there is a conflict between the legislation applicable to it and this Policy, the Chief Privacy Officer will make a responsible decision on the action to take and where appropriate will consult the ICO in case of doubt.

Rule 16C - Where Fluor receives a legally binding request from a law enforcement agency or state security body for disclosure of personal data transferred outside the UK under this Policy, Fluor will, unless prohibited from doing so, put the request on hold and promptly notify the ICO such notification to include information about the data requested, the requesting body and the legal basis for the disclosure.

Where Fluor receives a legally binding request for disclosure of personal data transferred outside the UK under this Policy and is prohibited from putting the request on hold and/or from notifying the ICO, Fluor will:

- use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as it can and as soon as possible to the ICO; and
- demonstrate to the ICO the steps it followed to deal with the request in accordance with this Policy.

Where Fluor is not able to notify the ICO, Fluor will provide to the ICO on an annual basis general information about the nature and number of such requests that it receives. Fluor will also ensure that any transfers that it makes to a public authority are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

PART III – APPENDICES

APPENDIX 1:
DATA SUBJECTS' RIGHTS REQUEST PROCEDURE

1. **Background**

UK data protection law gives data subjects whose personal data is processed in the UK certain rights as enumerated below Data subjects whose personal data is transferred between or among Fluor entities under this Policy will also benefit from these rights. This Data Subject Rights Request Procedure explains how Fluor deals with data subject rights relating to such personal data (referred to as a "valid request" in this Procedure).

1.1 A data subject making a valid request to Fluor is entitled to exercise the following rights:

(a) be informed by Fluor whether their personal data is being processed by Fluor (this is known as the right of 'subject access'); and

(b) rectify, erase, restrict, or port, and/or to object to the processing of, their personal data.

1.2 Information about how data subjects may exercise the rights described above is also contained in the privacy notices provided to data subjects by Fluor.

1.3 Requests from data subjects relating to the rights described above may be made in writing (which can include email) or orally. Where an oral request is made, Fluor will document the request and provide a copy to the data subject making the request before dealing with it. Requests made by employees should be directed to their supervisor or to a local HR representative. Requests made by third parties should be directed to a local HR representative or the project information manager, as appropriate. Written requests should be identified as a "Data Subject Rights Request" in the subject line. Requests which are not so identified, but which are nonetheless reasonably identifiable as valid requests, shall be treated as valid requests.

2. **Data subjects' Rights:**

2.1 A data subject making a valid request to Fluor is entitled, as appropriate, to:

(a) be informed whether Fluor is processing personal data about them;

(b) be given a description of:

(i) the purposes for which the personal data is being processed and the categories of personal data concerned;

(ii) the recipients or categories of recipient to whom their personal data is, or may be, disclosed by Fluor, including recipients located outside the UK;

(iii) the safeguards in place where personal data is transferred from the UK to a third country;

(iv) the logic involved (to the extent required by applicable law), significance, and consequences of any processing undertaken by automatic means, including profiling;

(v) be advised, where possible, about the period for which the personal data will be stored, or the criteria used to determine that period; and informed about the rights to rectification, erasure, restriction, objection and to complain to the ICO;

(vi) be given details about the source of the personal data if it was not collected from the data subject;

(c) where the valid request is for subject access, receive a copy of their personal data held by Fluor. If the request is made by email, the information shall be provided via email, unless the data subject making the request indicates otherwise;

(d) where the valid request is for data portability where the processing is based on solely on the grounds of a legal contract or consent and not on the grounds of legitimate interest of Fluor or compliance with legal obligations in the field of employment by a person who has provided their personal data to Fluor, receive that personal data in a structured, commonly used and machine-readable format and, if required and technically feasible, have it transmitted to another controller;

(e) require the rectification, erasure, restriction, or completion of their personal data; and/or

(f) object to the processing of their personal data.

The information listed above in items (a), (b) and (d) is contained in the privacy notices provided to data subjects by Fluor.

2.2 Under normal circumstances no fee will be applied to valid requests unless, in the reasonable opinion of the Chief Privacy Officer, Fluor is able to demonstrate that the request is manifestly unfounded or excessive, in which case Fluor may charge a reasonable fee.

2.3 Fluor must respond to a valid request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. Fluor shall inform the data subject of any such extension within one month of the receipt of the request, together with the reasons for delay. Requests made electronically shall be responded to electronically, where possible, unless requested otherwise.

2.4 If Fluor does not take action on a request, it shall inform the data subject without delay at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the ICO and seeking a judicial remedy.

2.5 Fluor is not obliged to comply with a subject access request unless Fluor is supplied with such information which it may reasonably require in order to confirm the identity of the data subject making the request and to locate the information which that person seeks.

3. **Receipt of a Request**

3.1 If any employee or subcontractor of Fluor receives any request from data subjects for their personal data or exercising any other rights under this Procedure, they must pass the communication to their supervisor or to a local HR representative upon receipt indicating the date on which it was received together with any other information which may assist that person in dealing with the request.

3.2 Any supervisor, local HR representative or project information manager receiving a request shall forward that request to the local designated data protection official, who shall be the local head of HR or his or her designee. In most cases, this will be the local data privacy ambassador.

3.3 The local designated data protection official will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

3.4 The local designated data protection official will contact the data subject in writing to confirm receipt of the request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions applies.

4. **Exemptions**

4.1 A valid request for access may be refused on the following grounds:

(a) If the refusal to provide the data is made in accordance with UK data protection law;

(b) Fluor demonstrates that the request is manifestly unfounded or excessive, and Fluor informs the data subject of the refusal of the request within one month of the receipt of the request, together with the reasons for not taking action and the data subject's right to complain to the ICO or seek a judicial remedy in relation to the refusal; or

(c) where the personal data does not originate from and has not been processed in the UK or is not otherwise subject to UK data protection law and requires Fluor to use disproportionate effort.

5. **The Search and the Response**

5.1 The local designated data protection official will arrange a search of all relevant electronic and paper filing systems. Typically, this will involve interaction with HR Data Privacy.

5.2 The local designated data protection official, or as applicable HR Data Privacy, may refer any complex cases to the Chief Privacy Officer for advice, particularly where the request relates to subject access and includes information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

5.3 Where the valid request is a request for subject access, the information requested will be collated by the local designated data protection official or his or her designee, or

HR Data Privacy as applicable, into a readily understandable format (internal codes or identification numbers used at Fluor that correspond to personal data shall be translated before being disclosed). A covering letter will be prepared in accordance with Fluor standard policies, procedures and forms, which includes information required to be provided in response to a subject access request.

5.4 Where the valid request is a request for data portability, the personal data requested will be collated into a structured, commonly used and machine-readable format and, at the request of the data subject and where technically feasible, transmitted to another controller.

5.5 If a request is received for the rectification, erasure, restriction or completion of personal data, such a request must be considered and dealt with as appropriate by the appropriate data protection official. In particular:

(a) If a request is received advising of a change or any inaccuracy in that data subject's personal data, such data must be rectified or updated accordingly if Fluor is satisfied that there is a legitimate basis for doing so.

(b) When, pursuant to a valid request, Fluor erases, anonymises, updates, or corrects personal data, the relevant Fluor entity will notify other Fluor entities that may be processing the personal data or any processor to whom the personal data has been disclosed accordingly so that they can also update their records.

(c) If the valid request is to erase that data subject's personal data in accordance with the provisions of UK data protection law, the matter will be assessed by the Chief Privacy Officer. Where the processing undertaken by Fluor is required by law or is necessary for the exercising of the right of freedom of expression and information, the request will not be regarded as valid.

(d) All queries relating to this Policy by employees are to be addressed to your supervisor, or the local head of HR, or HR Data Privacy as applicable, or if further clarification is required thereafter, to the Chief Privacy Officer, or for third parties, directly to the local HR representative or the project information manager, as appropriate.

BINDING CORPORATE RULES POLICY, APPENDIX 2: AUDIT PROTOCOL

1. Background

The purpose of the Data Protection Binding Corporate Rules Policy ("Policy") is to safeguard personal data transferred between Fluor entities. One of the requirements of the ICO is that Fluor audits compliance with the Policy and satisfies certain conditions in so doing and this document describes how Fluor deals with such requirements.

One of the roles of Fluor's Chief Privacy Officer is to provide guidance about the processing of personal data subject to the Policy and to assess the processing of personal data by Fluor for potential privacy-related risks. The processing of personal data with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. In addition, audits of other aspects of the business (e.g. IT systems or SOX compliance) also cover aspects of privacy compliance.

This Audit Protocol describes the formal assessment process adopted by Fluor to ensure compliance with the Policy as required by the ICO in addition to, but distinct from, the on-going day-to-day oversight of privacy compliance that falls within the responsibility of Fluor's Chief Privacy Officer.

2. Approach

2.1 Scope of audit

Fluor's Chief Privacy Officer will ensure that audits adequately address all aspects of the Policy, reflecting a **risk-based approach**. The risk assessment is based among other things upon input provided by the local data privacy officers, the Information Security department, the Internal Audit Department, Business Controls, and individual business lines. The relevant criteria to be considered in the risk assessment will include: the magnitude of the risk to Fluor employee data privacy rights in relation to the likelihood of occurrence, the areas of current regulatory focus, past experience, areas with changes to the systems or processes used to safeguard personal data, areas where there have been previous audit findings or complaints since the last review and the nature and location of the personal data processed.

Audits shall cover all aspects of the Policy and the processing undertaken by Fluor including: IT applications and systems, handling of data by third party processors and controllers, contractual terms applicable to such parties and physical data handling processes and procedures by local offices and local projects.

Fluor's Chief Privacy Officer will be responsible for ensuring that any issues or instances of non-compliance that are identified to the Chief Privacy Officer as a result of an independent internal or external audit are brought to the attention of Fluor's department of Internal Audit, Chief Legal Officer, Head of Human Resources, and Head of Compliance, as appropriate, and will provide a briefing of the results of the

audit, and the parties shall discuss any issue identified and take appropriate steps to ensure that any corrective actions required take place.

In addition, the Fluor Internal Audit Department has responsibility to undertake periodic audits of the Fluor Global data privacy program, including compliance with GDPR and UK law, as well as other applicable global data privacy law. Fluor Internal Audit operates independently of the Chief Privacy Officer, insofar as the Chief Privacy Officer and the data privacy program are in fact the subject of the audit, but at its discretion, Internal Audit consults with the Chief Privacy Officer to assist it in its audit activities. The Chief Privacy Officer supports and consults with Internal Audit on the scope of the audit, and reviews the results of the audit.

Further, Fluor Information Technology has an IT Compliance/Business Controls unit which assesses data privacy compliance insofar as this is necessary for Fluor, as a public company, to maintain adequate controls over its financial systems and reporting, for purposes of compliance with applicable law.

2.2 Any items which are deemed material in nature to the operation of a particular business line as a whole are be reported to the Group Executive level, and the Group Executives shall report matters material to Fluor as a whole to the Board of Directors.

2.3 Timing

Audits of the Policy will take place at least annually, or at the instigation of Fluor's Chief Privacy Officer, and typically occur on an ongoing basis. Audits of certain aspects of the Policy shall take place as needed if it is deemed by the Chief Privacy Officer, or other appropriate functions as described below, in consultation with the applicable business unit or office, that a more immediate audit is necessary or advisable.

2.4 Auditors

Audits of the Policy will be coordinated by Fluor's Chief Privacy Officer or his or her designees, and by the Internal Audit Department for which the Chief Privacy Officer shall provide support.. The Chief Privacy Officer may rely on work performed by accredited independent internal or external auditors, or speciality data privacy consultancies, to fulfil Fluor's audit obligations or by other supporting departments with an audit function, such as Information Security, IT Compliance/Business Controls, or the Internal Audit Department, as each function deems appropriate in the interest of overall data privacy and security. Fluor's Chief Privacy Officer, in consultation with the Internal Audit Department, or other supporting departments, such as Information Security or IT Compliance/ Business Controls, in consultation with such Officer or independently, as each function deems appropriate in the interest of overall data privacy and security, will provide quality assurance of audit work performed by others.

2.5 Report

Fluor has agreed to provide copies of the results of any audit of the Policy to the ICO upon written request subject to applicable law and respect for the confidentiality and trade secrets of the data provided. Fluor's Chief Privacy Officer will be responsible for liaising with the ICO for this purpose.

2.6 Audit by the ICO

In addition, Fluor has agreed to be audited by the ICO, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the data obtained and to the trade secrets of Fluor. Fluor shall assign Fluor personnel or an independent audit firm to work with the ICO for purposes of planning and implementing the audit. Fluor's Chief Privacy Officer will also be responsible for liaising with the ICO for this purpose. Where appropriate, the Chief Privacy Officer will report results or findings to the heads of Internal Audit, Human Resources, the Legal Department, or Compliance to coordinate remediation of audit findings.

BINDING CORPORATE RULES POLICY, APPENDIX 3: COMPLAINT HANDLING PROCEDURE

Background

The Policy safeguards personal data transferred between Fluor entities. The content of the Policy is determined by the ICO, and one of its requirements is that Fluor must have a complaint handling procedure in place. The purpose of this procedure is to explain how complaints brought by a data subject whose personal data is subject to this Policy are dealt with.

How data subjects can bring complaints/who handles complaints

Data subjects who know, or have a reason to suspect, incidents of inappropriate handling or other processing of their personal data may discuss the matter with the persons involved, or report the circumstances to their supervisor, local Human Resources manager, or at their election, to the independent ethics hotline (to the extent allowed by local law) or the Chief Privacy Officer by email to chief.privacy.officer@fluor.com or in writing to 6700 Las Colinas Blvd. Irving, TX 75039 USA.

What is the response time?

Unless exceptional circumstances apply (for example, as a result of disrupted communications due to the remote location of a project office), the applicable investigating personnel will acknowledge receipt of a complaint to the data subject concerned within 3 business days, investigating and providing a response within one month. This one month period may be extended at maximum by two further months (e.g due to the complexity of the complaint) provided that the complainant is informed of the reason for the time extension within one month of making the complaint.

When a complainant disputes a finding

If the complainant disputes the response of the investigating department, or any aspect of a finding and notifies their contact with the investigative staff, the matter will be referred to the Chief Privacy Officer within three business days, who will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The Chief Privacy Officer will respond to the complainant within one month of the referral. As part of the review the Chief Privacy Officer may arrange to meet the parties in an attempt to resolve the complaint.

If the complaint is upheld, the Fluor Chief Privacy Officer, in consultation with the investigating department and the head of Compliance, will arrange for any necessary steps to be taken as a consequence.

Data subjects whose personal data is processed in accordance with UK data protection law under this Policy have rights under the Policy to complain to the ICO and/or to make a claim against the Fluor entity that was responsible for exporting their personal data in a court in the UK if they are not satisfied with the way in which the complaint has been resolved. Data subjects entitled to such rights will be notified accordingly as part of the complaint handling procedure.

BINDING CORPORATE RULES POLICY, APPENDIX 4: COOPERATION PROCEDURE

This Binding Corporate Rules Policy Co-operation Procedure sets out the way in which Fluor will co-operate with the ICO in relation to this Policy.

The Fluor Chief Privacy Officer shall be the lead for all purposes of dealing with the ICO on data privacy matters, and may involve local Fluor data privacy officers as appropriate.

The Chief Privacy Officer shall ensure that any advice received from the ICO is communicated to the Law Department and to Corporate Compliance as appropriate.

Where required, Fluor will make the necessary personnel available for dialogue with the ICO in relation to the Policy.

As part of this dialogue, Fluor will actively review and consider: (1) any decisions made by the ICO on any data protection law issues that may affect the Policy; and (2) the views of the ICO as outlined in its published UK guidance on Binding Corporate Rules for controllers and processors.

Fluor has agreed to provide copies of the results of any audit of the Policy to the ICO subject to applicable law and respect for the confidentiality and trade secrets of the data provided. In addition, Fluor agrees that that the ICO may audit the Fluor entities for the purpose of reviewing compliance with the Policy on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the data obtained and to the trade secrets of Fluor.

Fluor agrees to abide by the advice of the ICO on any issues related to the interpretation and application of the Policy where a right of appeal is not exercised.

BINDING CORPORATE RULES POLICY, APPENDIX 5: UPDATING PROCEDURE

This Updating Procedure sets out the way in which Fluor will communicate changes to this Policy to the ICO, data subjects and to the Fluor entities bound by the Policy.

Fluor shall communicate any substantive changes to the Policy to the ICO as soon as reasonably practicable. Fluor will communicate changes to the Policy which are administrative in nature or which have occurred as a result of a change of UK data protection law through any legislative, court or ICO measure at least once a year. Fluor will also provide a brief explanation of the reasons for any notified changes to the Policy. Fluor will communicate any changes to the Policy to the Fluor entities bound by the Policy and to the data subjects who benefit from the Policy by periodically publishing revised versions of this Policy and applicable supporting policies on the Fluor intranet and at https://www.fluor.com/SiteCollectionDocuments/fluor-data-protection-policy.pdf. The Chief Privacy Officer will maintain a record of any updates to the Policy.

Fluor, as a reporting public company, maintains an up to date list of all Fluor entities through a corporate officer located in its headquarters office. Fluor shall ensure that all new Fluor entities are bound by and can deliver compliance with the Policy before a transfer of personal data to them takes place. Fluor will communicate changes to the list of Fluor entities once a year to the ICO. Otherwise, Fluor will communicate an up to date list of entities to the ICO when required.

APPENDIX 6
Processing Schedule

The Controller (as defined in Part 1 of this Processing Schedule ("Part 1")) wishes to appoint the Processor (also as defined in Part 1) to process certain personal data on its behalf in accordance with Rule 4C of the Policy. The Controller and the Processor have elected to complete this Processing Schedule as the means by which to satisfy the requirements of UK data protection law, and will comply with the requirements of this Schedule which is binding on the Controller and the Processor under the BCR Policy ("Policy"), and is to be read and interpreted in conjunction with the Policy.

Part 1: Processing Instructions

1.1. Name of Fluor entity as controller: ……...……(the "Controller")

1.2 Name of Fluor entity as processor: ……..……(the "Processor")

1.3 Purpose of the processing carried out by the Processor: …….....

1.4 The information processed will include the following categories of personal data:

(a) [list each category of personal data that will be processed, e.g. names, email addresses, financial information]

1.5. The data subjects to whom the personal data relate are:

(a) [list each category of data subjects, e.g. employees]

1.6. The activities to be carried out by the Processor on behalf of the Controller will consist of:

(a) [describe services carried out by the Processor on the Controller's behalf in detail]

1.7. Duration of processing carried out by the Processor: …….....

Part 2: Processor's Obligations

2. The Processor shall:

2.1 ensure that personnel/contractors authorised to process the personal data described in Part 1 (the "Data") have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.2 inform the Controller: (a) of the relevant legal requirement if it is legally required to process the Data otherwise than as instructed by the Controller before such processing

occurs, unless the law requiring such processing prohibits the Processor from notifying the Controller on important grounds of public interest, in which case it will notify the Controller as soon as that law permits it to do so; and (b) immediately about any instruction from the Controller which, in the Processor's opinion, infringes UK data protection law;

2.3 not subcontract any processing of the Data or otherwise disclose the Data to any third party except as authorised by the Controller in writing. Where sub-contracting is permitted the Processor will: (a) ensure that it has a written contract (the "Processing Subcontract") in place with the relevant subcontractor which imposes on the subcontractor the same obligations in respect of processing of the Data as are imposed on the Processor under Rule 4C and this Part 2 to the Processing Schedule ("Part 2"); (b) ensure that there are sufficient guarantees in place to ensure the Processing Subcontract meets the requirements of Article 28 of the UK GDPR; (c) remain fully liable to the Controller for its obligations under Rule 4C and this Part 2; and (d) ensure that Rule 6 of the Policy is complied with in the event that Data is subject to a trans-border transfer to a sub-contractor;

2.4 upon completion of the processing carried out by the Processor on the Controller's behalf and at the choice of the Controller, return or delete all Data processed by the Processor and all copies of such information unless the Processor is prevented from doing so by UK law, in which case the Data will be kept confidential and will not be actively processed for any purpose; and

2.5 provide such information, co-operation and assistance as the Controller reasonably considers to be necessary to enable the Controller to: (a) verify Processor's compliance with Rules 4A and 4C of the Policy and this Processing Schedule, including allowing for and contributing to audits and inspections by the Controller or another auditor mandated by the Controller; (b) carry out prior assessments of processing activities which are likely to result in a high risk to the rights and freedoms of data subjects and any related consultations with competent Supervisory Authorities; (c) fulfil its obligations in respect of any request by data subjects to exercise their rights under the Policy, including by notifying the Controller without undue delay of any such request; and (d) investigate, mitigate and notify in accordance with Rule 4D of the Policy any Data Protection Breach involving the Data, including by notifying the Controller without undue delay of any such Data Protection Breach.