Fluor 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 European data protection law and specifically to transfers of personal information collected and used in Europe between the Fluor entities.

This Policy applies to all Fluor entities and their employees and contains 15 rules ("Rules"). Fluor employees must comply with and respect this Policy when handling personal information collected and used in Europe. This Policy does not replace any specific data protection requirements that might apply to a specific business area or function.

This Policy applies to personal information of Fluor employees, and those of its clients, business or contracting partners, suppliers or other third parties, collected and used in Europe as part of the regular business activities of Fluor. Transfers of this personal information take place between the Fluor entities during the normal course of business and such information may be stored in centralised databases accessible by Fluor entities from anywhere in the world.

Scope

"Personal information", for purposes of this Policy, includes any information which relates to an identified or an identifiable person.

For purposes of this policy, "Europe" includes the European Economic Area (Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom) and Switzerland.

This Policy binds all Fluor entities and their respective employees worldwide. All Fluor entities and all Fluor personnel must comply with this Policy when handling personal information collected and used in Europe.

Policy Access

This Policy is published on the Fluor intranet accessible on OneFluor's Career & Life Resources page within the HR Toolkit, Practices, Information Privacy and Security, Fluor Data Protection Binding Corporate Rules Policy and on the Fluor website accessible at www.fluor.com/legal

BACKGROUND

WHAT IS DATA PROTECTION LAW?

Data protection law gives people the right to control how their personal information is used, and establishes restrictions on how that information may be collected, used, stored, and transmitted. When Fluor collects and uses the personal information of its employees, or those of its clients, business or contracting partners, suppliers or other third parties, this collection and use is covered and regulated by data protection law, and in particular, by the data protection law of the European Union.

HOW DOES DATA PROTECTION LAW AFFECT FLUOR INTERNATIONALLY?

Data protection law in a particular jurisdiction can impact how Fluor and its employees can handle information worldwide. For example, European data protection law does not allow the transfer of personal information to countries outside Europe 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 European data protection authorities as providing an adequate level of protection for individuals' 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 information in its possession is handled securely, and that its privacy is maintained. This Policy and the appendices also ensure that personal information is handled consistent with the law of all jurisdictions in which Fluor operates. The purpose of this Policy is to set out a general framework to satisfy the standards contained in European data protection law so as to provide an adequate level of protection for all personal information used and collected in Europe and transferred from the Fluor entities within Europe to Fluor entities outside Europe.

Central to this Policy are 15 Rules based on, and interpreted in accordance with, relevant European 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 INFORMATION COLLECTED AND USED?

Employees of Fluor and of its clients, business or contracting partners, suppliers or other third parties whose personal information is collected and used in Europe and is then transferred to Fluor entities outside Europe benefit from certain additional rights to enforce the Rules set out in this Policy. These individuals have the right to*:*

- seek to enforce compliance by Fluor with this Policy, including its appendices;

- lodge a complaint with a European data protection authority of competent jurisdiction and/or to take action in the applicable local jurisdictional courts against the Fluor entity established in Europe and responsible for exporting the personal information (the "Exporting Fluor EU Entity") in order to enforce compliance with this Policy, including its appendices;

- complain to an Exporting Fluor EU Entity, seek appropriate redress from the Exporting Fluor EU Entity, including the remedy of any breach of the Policy by any Fluor entity outside Europe and, where appropriate, receive compensation from the Exporting Fluor EU 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 authority;

- obtain a copy of this Policy and any unilateral declaration made by Fluor in connection with this Policy.

In the event of a claim being made in which an individual has suffered damage where that individual 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 Europe is not responsible for the breach, or that no such breach took place, will rest with the Exporting Fluor EU Entity.

Fluor has appointed a Chief Privacy Officer as the person to oversee and ensure compliance with this Policy. The Chief Privacy Officer works in active cooperation with Legal, Human Resources, Compliance, and /or data privacy officers at the regional and country level who are responsible for overseeing and enabling compliance with this Policy on a day-to-day basis.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues you can 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.

Steven Quevedo **Chief Privacy Officer** **EU +44 1252 29 1873** **US 949 349 7906** **US 864 281 8078** **steven.quevedo@fluor.com** **100 Fluor Daniel Drive, C102B** **Greenville, SC 29607** **USA**
Wendy Hallgren **Chief Compliance Officer** **469 398 7000** **wendy.hallgren@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 individuals whose personal information is processed by Fluor.

If you are concerned about the way in which Fluor has used your personal information, 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 European data protection law which Fluor must observe when Fluor collects and uses personal information in Europe.

Section B deals with the practical commitments made by Fluor to the European data protection authorities in connection with this Policy.

Section A Basic Principles of European Data Protection Law

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1 – 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 information (namely, local law implementing the EU Data Protection Directive 95/46/EC) and will ensure that where personal information is collected and used in Europe this is done in accordance with local 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 information subject to the Policy adhering to the Rules in this Policy.

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

Rule 2A – Fluor will explain to individuals, at the time their personal information is collected, how that information will be used.

Fluor will ensure that individuals are always told in a clear and comprehensive way (usually by means of a fair processing statement) about the uses and disclosures made of their personal information (including the secondary uses and disclosures of the information), the recipients or categories of recipients of the personal information and the identity of the data controller when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that. Where Fluor has obtained individuals' personal information from a source other than that individual, Fluor will provide this information to the individual when the information is first recorded 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 law).

Rule 2B – Fluor will only obtain and use personal information for those purposes which are known to the individual or which are within their expectations and are relevant to Fluor.

This rule means that Fluor will identify and make known the purposes for which personal information will be used (including the secondary uses and disclosures of the information) when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so as described in Rule 2A.

Rule 2C – Fluor will only change the purpose for which personal information is used if Fluor makes individuals aware of such changes or it is within individuals' expectations and they can express their concerns.

If Fluor collects personal information for a specific purpose (as communicated to the individual via the relevant fair processing statement) and subsequently Fluor wishes to use the information for a different or new purpose, the relevant individuals will be made aware of such a change unless;

- it is within their expectations and they can express their concerns; or
- there is a legitimate basis for not doing so as described in Rule 2A above.

In certain cases, for example, where the processing is of sensitive personal information, or Fluor is not satisfied that the processing is within the reasonable expectation of an individual, the individual's consent to the new uses or disclosures may be necessary.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – Fluor will keep personal information accurate and up to date.

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

Rule 3B – Fluor will only keep personal information for as long as is necessary.

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 keep personal information which is adequate, relevant and not excessive.

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

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – Fluor will always adhere to its IT Security Policies.

Fluor will comply with the requirements in applicable information security and personal private and financial information handling policies that apply company-wide and, as applicable, to a particular office or function, as revised and updated from time to time

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

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

Rule 4C- Where Fluor entities process personal information 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 information on behalf of another Fluor entity, the Fluor service provider must act only on the instructions of the Fluor entity on whose behalf the processing is carried out and ensure that it has in place proportionate technical and organizational security measures to safeguard the personal information.

RULE 5 – HONORING INDIVIDUALS' RIGHTS

Rule 5A – Fluor will adhere to the Subject Access Request Procedure.

Individuals are entitled (by making a written request to Fluor) to be supplied with a copy of personal information held about them (including both electronic and paper records). Fluor will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) when dealing with requests from individuals for access to their personal information.

Rule 5B – Fluor will deal with requests to delete, rectify or block inaccurate personal information or to cease processing personal information in accordance with the Subject Access Request Procedure.

Individuals are entitled to request rectification, deletion or blocking, as appropriate, of their personal information which is shown to be inaccurate and, in certain circumstances, to object to the processing of their personal information. Fluor will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR OVERSEAS TRANSFERS

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

In principle, international transfers of personal information to third parties outside the Fluor entities are not allowed without appropriate steps being taken, such as signing up to Model or contractual clauses, or adherence to applicable Safe Harbor principles, which will protect the personal information being transferred.

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 7A – Fluor will only use sensitive personal information if it is absolutely necessary to use it.

Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. Fluor will assess whether sensitive personal information is required for the proposed use and when it is absolutely necessary in the context of the business.

Rule 7B – Fluor will only use sensitive personal information where the individual's express consent has been obtained unless Fluor has an alternative legitimate basis

for doing so.

In principle, individuals must expressly agree to the collection and use of their sensitive personal information by Fluor unless Fluor has a legitimate basis for doing so. This permission to use sensitive personal information by Fluor must be genuine and freely given.

RULE 8 – LEGITIMIZING DIRECT MARKETING

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

All individuals have the data protection right to object to the use of their personal information for direct marketing purposes and Fluor will honor all such opt out requests.

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 - Where decisions are made by automated means, individuals will have the right to know the logic involved in the decision and Fluor will take necessary measures to protect the legitimate interests of individuals.

There are particular requirements in place under European data protection law to ensure that no evaluation of or decision about an individual which significantly affects them can be based solely on the automated processing of personal information unless measures are taken to protect the legitimate interests of individuals.

SECTION B PRACTICAL COMMITMENTS MADY BY FLUOR

RULE 10 – TRAINING

Rule 10 – Fluor will provide appropriate training to employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools used to process personal information.

RULE 11 – AUDIT

Rule 11 – Fluor will comply with the Binding Corporate Rules Policy Audit Protocol set out in Appendix 2.

RULE 12 – COMPLAINT HANDLING

Rule 12 - Fluor will comply with the Binding Corporate Rules Policy Complaint Handling Procedure set out in Appendix 3.

RULE 13 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 13 – Fluor will comply with the Binding Corporate Rules Policy Co-operation Procedure set out in Appendix 4.

RULE 14 – UPDATE OF THE RULES

Rule 14 – Fluor will comply with the Binding Corporate Rules Policy Updating Procedure set out in Appendix 5.

RULE 15 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 15A – 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 its ability to comply with the Policy, Fluor will promptly inform the Chief Privacy Officer unless otherwise prohibited by a law enforcement authority.

Rule 15B – 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 will consult the data protection authority with competent jurisdiction in case of doubt.

PART III – APPENDICES

APPENDIX 1 SUBJECT ACCESS REQUEST PROCEDURE

APPENDIX 2 AUDIT PROTOCOL

APPENDIX 3 COMPLAINT HANDLING PROCEDURE

APPENDIX 4 CO-OPERATION PROCEDURE

APPENDIX 5 UPDATING PROCEDURE

APPENDIX 1:
SUBJECT ACCESS REQUEST PROCEDURE

1.1 Background.

European Data Protection law gives individuals whose personal information is collected and used in Europe the right to be informed whether any personal information about them is being processed by an organization. This is known as the "right of subject access." Individuals whose personal data is collected and used in Europe and transferred outside Europe between Fluor entities under the Fluor Binding Corporate Rules Policy will also benefit from this right. This Subject Access Procedure explains how Fluor deals with a subject access request relating to such personal information (referred to as "valid request" in this Procedure).

2. Subject Access Procedure

2.1 An individual making a valid request to Fluor is entitled to:

(a) Be informed whether Fluor holds and is processing personal information about that person.

(b) Be given a description of the personal information, the purposes for which they are being held and processed and the recipients or classes of recipient to whom the information is, or may be, disclosed by Fluor.

(c) Communication in intelligible form of the personal information held by Fluor.

2.2 The request must be made in writing, which can include email, and should be directed to your supervisor or to a local HR representative or, for third parties, to the local HR department. It should identify itself as a "Subject Access Request" in the re line. Requests which are not so identified, but which are nonetheless reasonably identifiable as valid requests, shall be treated as valid requests.

2.3 Under normal circumstances no fee will be applied to valid requests.

2.4 Fluor must respond to a valid request within 40 calendar days of receipt of that request.

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 individual making the request and to locate the information which that person seeks.

3. Receipt of a Subject Access Request

3.1 If any employee or subcontractor of Fluor receives any request from an individual for their personal information, 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 or local HR representative receiving a subject access 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.

4. Initial Steps

4.1 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.

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

5. Exemptions to subject access

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

(a) Where the subject access request is made to a European Fluor entity and relates to the use or collection of personal information by that entity, if the refusal to provide the information is consistent with the data protection law within that jurisdiction; or

(b) Where the subject access request does not fall within 4.1 (a) and

(i) if, in the opinion of Fluor it is necessary to do so to safeguard the legitimate business interests of Fluor, national or public security, defense, the prevention, investigation, detection and prosecution of criminal offences, for the protection of the data subject or of the rights and freedoms of others; or

(ii) if the personal information is held by Fluor in non-automated form and is not or will not become part of a filing system; or

(iii) where the provision of the personal information does not originate from and has not been processed in Europe and requires Fluor to use disproportionate effort.

6. The Search and the Response

6.1 The local designated data protection official will arrange a search of all relevant electronic and paper filing systems.

6.2 The local designated data protection official may refer any complex cases to the Chief Privacy Officer for advice, particularly where the request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.

6.3 The information requested will be collated by the local designated data protection official or his or her designee 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 by local designated data protection official in accordance with Fluor standard policies, procedures and forms, which includes information required to be provided in response to a subject access request.

6.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort there is no obligation to provide a copy of the information. The other information referred to in 1.1 above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

7. Requests for erasure, amendment or cessation of processing of information

7.1 If a request is received for the deletion of that individual's personal information, such a request must be considered and dealt with as appropriate by the local designated data protection official.

7.2 If a request is received advising of a change in that individual's personal information, such information must be rectified or updated accordingly if Fluor is satisfied that there is a legitimate basis for doing so.

7.3 If the request is to cease processing that individual's personal information because the rights and freedoms of the individual are prejudiced by virtue of such processing by Fluor, or on the basis of other compelling legitimate grounds, the matter will be referred by the local designated data protection official to the Chief Privacy Officer to assess. Where the processing undertaken by Fluor is required by law, the request will not be regarded as valid.

7.4 All queries relating to this policy are to be addressed to your supervisor, or the Head of Local HR, or if further clarification is required thereafter, to the Chief Privacy Officer, or for third parties, to the local HR department.

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 information collected and used in Europe which is transferred between Fluor entities. The Policy requires approval from the data protection authorities in the European member states from which the personal information is transferred. One of the requirements of the data protection authorities 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 collection and use of personal information subject to the Policy and to assess the collection and use of personal information by Fluor for potential privacy-related risks. The collection and use of personal information 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. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Fluor to ensure compliance with the Policy as required by the data protection authorities, this is only one way in which Fluor ensures that the provisions of the Policy are observed and corrective actions taken as required.

2. Approach

2.1 Scope of audit

Fluor's Chief Privacy Officer will be responsible for performing or coordinating the audits and will ensure that such audits address all aspects of the Policy. The scope of the audit performed annually will be decided by Fluor's Chief Privacy Officer taking 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, 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 information, areas where there have been previous audit findings or complaints,

the period since the last review the nature and location of the personal information 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, 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 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 provide a briefing of 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.

2.2 Any items which are deemed material in nature to the operation of a particular business line as a whole shall 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

Audit of the Policy will take place at least annually, or at the instigation of Fluor's Chief Privacy Officer. Audits of certain aspects of the Policy shall take place as needed if it is deemed by the Chief Privacy Officer, in consultation with the applicable business unit or office, that a more immediate audit is necessary or advisable.

2.4 Auditors

Audit of the Policy will be overseen by Fluor's Chief Privacy Officer or his or her designees, and reliance on work performed by other accredited internal or external auditors may be determined by such Officer. Fluor's Chief Privacy Officer, in consultation with the Audit Department, will manage and 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 a European data protection authority of competent jurisdiction upon written request subject to applicable law and respect for the confidentiality and trade secrets of the information provided. Fluor's Chief Privacy Officer will be responsible for liaising with the European data protection authorities for this purpose.

2.6 Audit by Data Protection Authorities

In addition, Fluor has agreed that where any Fluor entity is located within the jurisdiction of a data protection authority based in Europe, the data protection authorities may audit the Fluor entities for the purpose of reviewing compliance with the Policy in accordance with the applicable law in the country in which the Fluor entity is located, or, in the case of a Fluor entity located outside Europe, in accordance with the applicable law of the European country from which the personal information is transferred under the policy, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Fluor. Fluor shall assign Fluor personnel or an independent audit firm to work with the data protection authorities for purposes of planning and implementing the audit. Fluor's data privacy officer will also be responsible for liaising with the European data protection authorities 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 information transferred between Fluor entities. The content of the Policy is determined by the data protection authorities in the European member states from which personal information is collected and processed in Europe, and one of their requirements is that Fluor must have a complaint handling procedure in place. The purpose of this procedure is to explain how complaints brought by an individual whose personal information is collected and processed in Europe by Fluor under the Policy are dealt with.

How individuals 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 information 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.

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 individual concerned within 3 business days, investigating and providing a response within one month.

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.

Certain individuals whose personal information is collected and/or used and in accordance with European data protection law have rights under the Policy to complain to a European data protection authority and/or to lodge an application with a court of competent jurisdiction if they are not satisfied with the way in which the complaint has been resolved. Individuals 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 European data protection authorities in relation to this Policy.

The Fluor Chief Privacy Officer shall be the lead for all purposes of dealing with European Union regulatory bodies 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 local data privacy regulators is communicated to the Law Department and to Corporate Compliance as appropriate.

Where required, Fluor will make the necessary personnel available for dialogue with a European data protection authority in relation to the Policy.

As part of this dialogue, Fluor will actively review and consider: (1) any decisions made by relevant European data protection authorities on any data protection law issues that may affect the Policy; and (2) the views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules.

Fluor will provide upon written request copies of the results of any audit of the Policy to a European data protection authority of competent jurisdiction subject to applicable law and respect for the confidentiality and trade secrets of the information provided.

Where any Fluor entity is located within the jurisdiction of a data protection authority based in Europe, Fluor agrees that that data protection authority may audit that Fluor entity for the purpose of reviewing compliance with the Policy, in accordance with the applicable law of the country in which the Fluor entity is located, or, in the case of a Fluor entity located outside Europe, in accordance with the applicable law of the European country from which the personal information is transferred under the Policy, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Fluor.

Fluor agrees to abide by any formal decision of the applicable data protection authority 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 European data protection authorities, data subjects and to the Fluor entities bound by the Policy.

Fluor shall communicate any substantive changes to the Policy to the Information Commissioner's Office of the United Kingdom and any other relevant European data protection authorities as soon as reasonably practicable. Fluor will communicate changes to the BCR which are administrative in nature or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority 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.

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 the Policy before a transfer of personal information to them takes place. Fluor will communicate any substantial changes to the list of Fluor entities once a year. Otherwise, Fluor will communicate an up to date list of entities to the ICO and any other relevant European data protection authorities when required.