ICF GDPE PROGRAM ROLES & RESPONSIBILITIES

DOCUMENT OWNER: DPT
DATE: 01/27/20

PRIVILEGED AND CONFIDENTIAL | PLEASE DO NOT EXTERNALLY DISTRIBUTE

DPT Legend:
Data Protection Officer (DPO) | Chief Information Security Officer (CISO) | Data Protection Team (DPT) | Data Protection Risk Manager (DPM) | Data Protection Coordinator (DPC)
Capitalized terms used in this document have the meanings outlined in Section 6 "Glossary Terms" of the Data Protection Procedure.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
1.	**Governance Structure**	Maintain Data Protection and ePrivacy strategy, policies, procedures and related resources through ICF Global Data Protection and ePrivacy (GDPE) program and document/demonstrate organizations' Data Protection and ePrivacy compliance. (DPO) Answer Data Protection and ePrivacy questions, review, address related matters, analyze and identify risks, possible options for risk mitigation, oversee compliance, undertake related audits, and provide any related training, in alignment with applicable Data Protection and ePrivacy regulations and in conjunction with the ICF GDPE program. (DPT)	Owner | Monitored by: DPT Contributors: CBS (HR | Corporate Marketing: Facilitate Communications in collaboration with DPT)
2.	**ICF GDPE Program Governance Assurance**	Ensure employees' acknowledgment and agreement with Data Protection and ePrivacy policies and procedures and ICF GDPE program. (DPM | DPC) Maintain and, where appropriate, improve processes; maintain awareness and monitor implementation of the correct processes; monitor, identify and propose actions to address possible issues or breaches; and identify and propose action to address non-compliance to DPO. (DPC) Monitor adherence to GDPE program requirements and ensure effective communication of risk analysis and responses. (DPO)	Owner: OG | CBS Group ☐ Review, adopt and adhere to ICF GDPE program. ☐ Support assurance and provide related documentation for ICF GDPE accountability purposes. NOTE: While members of the DPT may manage or communication actions under the ICF GDPE program, the DPO is the designated program official under the regulatory requirements responsible for program determinations.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
3.	**Data Protection Policy & Procedure**	Maintain a Data Protection and ePrivacy policy and procedure. (DPO)	Owner: OG | CBS Group ☐ Adhere to and support and document compliance with the ICF GDPE program.
4.	**Training & Awareness**	Develop plans for and deliver Data Protection and ePrivacy training and awareness communications. (DPO | DPM | DPC)	Owner: HR ☐ Incorporate Data Protection and ePrivacy training into corporate learning and development for target user groups (e.g., HR, security, call center and etc.) using content developed by DPT Owner: OG | CBS Group - Primary Training Areas: ☐ Identification of Personal Data under control by a project team or group. ☐ Understanding of how and why Personal Data Processing is taking place. ☐ Understanding permissible use of Personal Data. ☐ Understanding protection of Personal Data. ☐ Identification of proper method for managing Data Subject requests. ☐ Identification of proper process for promptly responding to suspected Personal Data Breaches.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
5.	**Personal Data Inventory & Work Flow**	Establish ICF GDPE framework for maintaining an inventory of key Personal Data holdings (what Personal Data is held and where). (DPO) Provide guidance for OG and CBS Groups to comply with ICF GDPE program framework for maintaining an inventory of key Personal Data holdings (what Personal Data is held and where). (DPT)	Owner: OG | CBS Group ☐ Identify Personal Data holdings by type (e.g., sensitive, confidential, public) based on the ICF GDPE and ISO policy framework. ☐ Establish and maintain documented process for implementing and managing technical, operational and administration measures for projects and/or initiatives that align with the ICF GDPE framework and contractual obligations for Data Protection and ePrivacy requirements. **NOTE**: Highest level standard must be maintained. ☐ Maintain Personal Data Processing register for projects and initiatives, which further enables inventory of Personal Data holdings. ☐ Ensure appropriate documentation of change management of the lifecycle of client or client customer data and user-generated content for assurance and other purposes and initiate privacy impact assessments (PIAs) for business change events. ☐ Provide documentation for audit and assurance purposes, including to demonstrate effectiveness of Personal Data handling practices. **NOTE:** DPO, CISO and DPT are prohibited by policies and procedures and are not in the position to attest to project or initiative level technical, operational, administrative or security controls, or approve related business risk.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
6.	**Embed Data Privacy by Design & Default Into Operations - Corporate Facing**	Establish and maintain policies and procedures for data processing or treatment, including, the, e.g., use of children and minors' Personal Data. (DPO)	Owner: CBS Group ☐ When developing business systems, solutions or other project processes that involve processing of Personal Data or touch upon direct marketing practices, consult and obtain early guidance from the DPT. ☐ Maintain documentation to reflect CBS Group's integration of the ICF GDPE program requirements into CBS Group's day-to-day data processing business activities (including any direct marketing practices) at the start of and throughout project or initiative (development of systems, tools, etc.) lifecycle. For example, consistent with the requirements of the EU Directive: ☐ Ensure accountability (demonstrate lawful, fair, transparent, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality (need to know and authorized), and resiliency) (Accountability Practices). ☐ Ensure establishment and implementation of adequate technical, operational, administrative practices (Data Protection Practices) to protect Personal Data and systems. ☐ Collaborate with Procurement to understand related contractual obligations to ensure regulatory, contractual and ICF GDPE program compliance when managing initiatives involve processing of Personal Data and obtain early guidance from the DPT.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples

7.	**Third Party Risk Management**	Establish and maintain data protection and ePrivacy provisions and requirements (such as DPA, SARs, etc.) for third parties (e.g., clients, ICF (Sub)Processors, and affiliates). (DPT)	Owner: C&A – Contracts & Procurement:
			☐ Maintain procedures to execute contracts or agreements with all ICF (Sub)Processors engaged to Process Personal Data in collaboration with DPT where DPT Key DPT Review & Risk Analysis Triggers in Section 3 of the Data Protection Procedures are activated (***See also*** the **C&A-Client Facing Data Protection KT Flow Chart** or **C&A-Procurement Facing Data Protection KT Flow Chart**.)
			☐ Verify compliance of ICF (Sub)Processor's Personal Data processing activities with CBS Group.
			☐ Verify compliance of ICF (Sub)processor's Personal Data processing activities with OG and C&A POC.
			☐ Apprise, in collaboration with applicable project or initiative POC, appropriate business (line of business leader, division leader, group leader, etc.), C&A-Client Facing, and C&A-Procurement or other key stakeholders of:
			  ☐ DPT Advisories that reflect, at minimum, Moderate or High DPT Risk Analysis Ratings.
			  ☐ any deviations from the DPT Advisories.
			☐ obtain, *before Staff or ICF (Sub)Processor Process Personal Data or an ICF signatories sign Contracts*, documented appropriate business (line of business leader, division leader, group leader, etc.), approvals or rejections when:
			  ☐ the related DPT Advisories reflect, at minimum, either a Moderate or High DPT Risk Analysis Rating.
			  ☐ any deviations from the DPT Advisories are intended or occur.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
	Third Party Risk Management…cont'd		☐ upload, *before Staff or ICF (Sub)Processor Process* Personal *Data*, to the applicable KT Questionnaire Section 1.15: ☐ appropriate business (line of business leader, division leader, group leader, etc.) stakeholder approvals or rejections concerning DPT Advisories include either Moderate or High DPT Risk Analysis Ratings. ☐ appropriate business (line of business leader, division leader, group leader, etc.) stakeholder approvals or rejections concerning any deviations from DPT Advisories ☐ the final executed Contract within five (5) business days of execution. Participant: Monitored by DPT | IA

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
8.	**Embed Data Privacy by Design & Default Into Operations – Client Facing**	Establish and maintain policies | procedures for data processing or treatment and use of children and minors' Personal Data. (DPO)	Owner: OG ☐ Collaborate with C&A POC to: ☐ implement contract review steps outlined Row A of Table 1 in Section 3 of the Data Procedure (***See also*** the C&A-Client Facing Data Protection KT Flow Chart or C&A-Procurement Facing Data Protection KT Flow Chart.) ☐ understand contractual obligations to ensure regulatory, contractual and ICF GDPE compliance when managing projects or initiatives that involve processing of Personal Data or touch upon direct marketing practices. ☐ obtain early guidance from the DPT. ☐ ensure receipt, review and action upon DPT Advisories throughout contract lifecycle. ☐ apprise appropriate business (line of business leader, division leader, group leader, etc.), C&A-Client Facing, and C&A-Procurement or other key stakeholders of: ☐ DPT Advisories that reflect, at minimum, Moderate or High DPT Risk Analysis Ratings. ☐ any deviations from the DPT Advisories. ☐ obtain, *before Staff or ICF (Sub)Processor Process Personal Data or an ICF signatories sign Contracts*, documented appropriate business (line of business leader, division leader, group leader, etc.), approvals or rejections when: ☐ the related DPT Advisories reflect, at minimum, either a Moderate or High DPT Risk Analysis Rating. ☐ any deviations from the DPT Advisories are intended or occur.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
	Embed Data Privacy by Design & Default Into Operations - Client Facing…cont'd		☐ upload, *before Staff or ICF (Sub)Processor Process* Personal *Data*, to the applicable KT Questionnaire Section 1.15: ☐ appropriate business (line of business leader, division leader, group leader, etc.) stakeholder approvals or rejections concerning DPT Advisories include either Moderate or High DPT Risk Analysis Ratings. ☐ appropriate business (line of business leader, division leader, group leader, etc.) stakeholder approvals or rejections concerning any deviations from DPT Advisories. ☐ the final executed Contract within five (5) business days of execution. ☐ Establish project team level Accountability Practices and Data Protection Practices or Compliance Plan necessary for protecting (in an equivalent manner to that of the Data Controller) the Personal Data being processed. If a conflict exists between client (Data Controller) and ICF GDPE program requirements or related practices, follow the more stringent of the two. ☐ Collaborate with C&A POC and Procurement POC to follow contractual obligations, especially regarding appointment of ICF (Sub)Processors. ☐ Provide services solely on Data Controller' documented instructions. ☐ Provide assistance to the Data Controller in complying with the rights of Data Subjects. ☐ Return or destroy Personal Data when no longer needed or at the end of the relationship. ☐ Provide any information needed by the Data Controller to assist them in demonstrating their Data Protection compliance.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
9.	**Information Security Risk Management: Corporate Systems**	Monitor data security compliance concerning acceptable use of information or resources and contribute to policies as warranted. (DPO)	Owner: ISO ☐ Establish and maintain acceptable use policy. ☐ Maintain technical and security measures (e.g., intrusion detection, firewalls and monitoring). ☐ Establish a central Personal Data register. ☐ Collaborate with DPO/DPM/DPC on security related monitoring or audits concerning Personal Data. Participant: Monitored by DPT | IA
10.	**Information Security Risk Management: Insider Threat**	Ensure integration of corporate data security measures into policies and procedures and evidence-based regulatory compliance regarding access to employees' company e- mail accounts, devices, etc. and protection of employees', as data subjects', related rights. (DPO)	Owner: ISO Collaborate with DPO on security related monitoring and Internal Audit with respect to audit concerning Personal Data. Contributors: CIT | ISO | HR Participant: Monitored by DPT | IA
11.	**Information Security Risk Management: Client Facing Security Assessment Reviews and/or Audits**	Monitor data security compliance as part of overall data protection program. (DPO | DPM | DPC)	Owner: ISO ☐ Help OG respond to client SARs and audits regarding corporate level security framework activities. ☐ Review OG's related responses regarding OG implementation of ICF GDPE program compliant processing activity and OG's integration of responses, as applicable, from OG and/or CBS POCs HR or other focus area components. Participant: Monitored by DPT | IA

PRIVILEGED AND CONFIDENTIAL | PLEASE DO NOT EXTERNALLY DISTRIBUTE

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
12.	**Privacy Statement: Corporate Facing**	Create and maintain data protection statements, cookie notices, etc. that detail the organization's Personal Data handling practices. (DPO)	Site Owner: DPT | Corporate Marketing ☐ Publish DPT reviewed privacy statements, consent forms, cookie notice or and other related content. On-location Owner: OG ☐ Provide notice by means of on-location signage, posters.
13.	**Privacy Statement, Information Sheets, Data Protection Communication Plan, etc.: Client Facing**	Establish and maintain data protection privacy statement, cookie notices, etc. framework templates; and collaborate with OGs for client facing tailoring purposes. (DPO | DPM | DPC)	Owner: OG: ☐ Integrate business practices into template to detail OGs project level Personal Data handling practices in collaboration with CIT, Web Team and other stakeholders. ☐ Publish DPT reviewed privacy statements, consent forms, cookie notice or and other related content. ☐ Provide DPT reviewed notice in marketing communications (e.g., sites, emails, flyers and offers).
14.	**Data Subject Access Request (DSAR) & Complaint Responses**	Create and maintain DSAR toolkit; investigate root causes of data protection complaints, analyze and provide related guidance for responses. (DPO)	Owner: OG ☐ Maintain evidence-based procedures to address complaints in line with DSAR toolkit and in collaboration with DPT.
15.	**Existing and New Operational Practices**	Establish and maintain PIA | DPIA guidelines and templates. (DPO) Identify, assess and advise on ways to mitigate or minimize data protection risks with data processing activities. (DPO | DPM | DPC)	Owner: OG ☐ Conduct PIAs | DPIAs for existing (including process changes) and new programs, systems, processes in collaboration with CIT | ISO. Participant: Monitored by DPT | IA

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
16.	**Data Protection Incident | Breach Management Program**	Establish and maintain a data protection incident | breach response plan. (DPO)	Owner: ISO ☐ Create initial plan draft and collaborate with OGC to finalize. ☐ Engage a forensic investigation team as applicable. Participant: Monitored by DPT | IA
17.	**Data Protection Incident | Breach Handling**	☐ Gather from OG or CBS Group background information and business activities regarding data privacy incident through SIR to meet accountability regulation requirements. (DPO | DPM | DPC) **NOTE**: Process is often facilitated through live discussion, but completion of SIR by OG or CBS Group is essential to documentation portion of process. ☐ Conduct an investigation based on staff's and/or ICF (Sub)processor' provided information or SIR. (DPT) ☐ Review applicable technical or system information. (DPO | CISO) ☐ Undertake a risk assessment of the incident or breach, taking into account key considerations, including those required by regulations (e.g., the potential harm to the data subjects(s); the sensitivity of the data; the volume of data, etc.) (DPO) ☐ Assist CBS Group to assess reporting requirements to data subjects, clients or others and review/draft related notifications to report incidents or breaches for CBS Group related to corporate-facing matters. (DPO | CISO) ☐ Assist OG to assess reporting requirements to data subjects, clients or others and review/draft related	Owner: OG ☐ Plays vital role and contributes to overall organization responsibility for data protection or ePrivacy compliance. ☐ Plays vital role in establishing, implementing and monitoring technical, operational and administration level data protection and ePrivacy good practice in compliance with the GDPE framework or contractual obligations developed with guidance from DPT. ☐ Report any loss, misuse, incident or related breach of Personal Data to the DPT. **NOTE**: While regulatory requirements typically identify a 72-hour reporting requirement, many ICF contracts establish a shorter time period (e.g., 24 hours); hence prompt/immediate internal escalation and reporting is often critical. ☐ Identify and designate knowledgeable OG or CBS Group members who must populate the SIR to provide DPT accurate, relevant, and other requested information related to the business-related activity and details and the incident (e.g., related agreements, nature of the breach, related client or sub-processor details and affected projects, affected data subjects, an indication as to the volume of records or material involved, applicable POCs, any of details or materials). **NOTE**: The DPT does not have the necessary project-related details, relevant contractual and project information/materials and other matters related to the incident.

	Data Protection & ePrivacy Management Categories	Owned by the DPT Activities – Examples	Activities Owned by Operational Group (OG) or Corporate Business Services (CBS) Group – Examples
	Data Protection Incident | Breach Handling…cont'd	notifications to report incidents or breaches for OG related to client-facing matters. (DPO | CISO) ☐ Identify and recommend changes to OG or CBS Group processes and practices to address findings and prevent future incident or breach. (DPO | CISO)	Owner: ISO ☐ Review and analyze data security and related artifacts and share related data security analysis and documentation, including for any internal or external reporting. Participant: Monitored by DPT | IA
18.	**Monitor DPT ICF GDPE program practices**	Monitor and report data protection management metrics. (DPO/DPM/DPC)	Owner: Internal Audit ☐ Conduct audits of the ICF GDPE program (i.e., operational audit of the DPT).
19.	**Monitor OG and CBS Group Implementation of ICF GDPE program**	Monitor and report data protection operational level implementation metrics. (DPO/DPM/DPC) Conduct audits of the ICF GDPE program (i.e., operational audit by the DPT).	Owner: OG | CBS ☐ Collaborate and respond to operational level audits of the ICF GDPE program (i.e., operational audit by the DPT).
20.	**Track External Criteria**	Identify ongoing data protection compliance requirements, e.g., law, case law, codes, etc. (DPO/DPM/DPC) Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes. DPO/DPM/DPC)	Owner: Board | IA | ELT