Data Protection

White Paper

icf.com

How ICF’s GDPR and Similar Data Protection Compliance Implementation Supports our Data Subjects and Clients

The EU General Data Protection Regulation (“GDPR”) Regulation (EC) 2018/1725, UK Data Protection Bill, California Consumer Privacy Act of 2018 (“CCPA”), and ever-evolving similar worldwide data protection regulations are significant game changers for organizations that process personal data. These regulations strengthen the rights of individuals and will lead to better data privacy and data security practices.

ICF welcomes these new data protection changes. We care about data protection, understand that it’s a human right, and see these regulatory changes as an opportunity to build on and further strengthen our existing data protection and ePrivacy practices. These regulatory changes will benefit individuals and organizations as they will increase trust between them. Through this journey, we will continue to maintain and enhance our data protection compliance.

We are sharing the content within this white paper to explain our data protection implementation approach.

What key steps is ICF taking to be compliant with GDPR and similar rigorous data protection and ePrivacy regulations and laws?

ICF is a global organization that both controls and processes personal data from around the world, including, for example, in the EU, Asia, Africa, and Canada. Our existing certifications and long-standing commitment to data protection frameworks prepare us for GDPR and similar regulations (e.g., CCPA, Canadian Data Privacy Statutes, etc.) in many ways.

Using the GDPR and GDPR-like regimes as our baseline, we generally have:

- Built on ICF's existing data protection experience and compliance mechanisms.
- Developed our Global Data Protection and ePrivacy (GDPE) program through an exhaustive and intensive process.
- Drafted a data protection policy, procedure, and related materials with in-house and external counsel, continuously refined the versions into specific and actionable general product requirements with detailed input from key company stakeholders, and subsequently translated the program materials into group-specific actions for each group.
- Nominated a Data Protection Officer ("DPO") who leads our GDPE program implementation and is supported by a dedicated data protection team, which includes ICF's DPO and Chief Information Security Officer ("CISO").
- Engaged the renowned law firm, DLA Piper, LLP, among several others, to support our GDPE program implementation.

Specific key steps for implementation

ICF's Global Data Protection and ePrivacy (GDPE) program implementation is focused on supporting your and our organization with implementation of the data protection regulations. A summary of our key steps includes:

1. Global Baseline Data Protection-ready measures:

Transparency

- Ability for clients to link service offerings to local geographic privacy statements/notices
- Provide information on how personal data is generally being used in a service or too

Data minimization / deletion

- Review of services for unnecessary personal data
- Review of services for opportunities to use pseudonymous or anonymous data instead of personal data
- Ability to delete personal data when data is no longer needed or requested by clients (where clients/ users cannot delete data themselves)

General individual rights

- Ability to provide access to and correct personal data when requested by clients or individuals
- Ability to delete personal data when requested by clients or individuals

EU individual rights

- Ability to deal with data subject access requests (e.g., data portability – individuals' right to receive their data in a machine-readable format)
- Ability to stop using personal data (right to object / right to restriction in certain circumstances)

2. **Embedded Privacy by Design and Default Measures Within Operations:** As it becomes more and more challenging in today's world for individuals to maintain control over their information, privacy by design and accountability becomes increasingly important to maintain the trust of individuals, clients, and regulators, and to document how an organization complies with the data protection regulations.

   As a result, we place our privacy by design and default ("PbD") approach at the heart of our GDPE program.

- Review and update our policies to embed and implement PbD checklist and process within our service lifecycles
- Functional areas and groups are including the PbD checklist into their change processes
- Implement PIA or DPIA process to facilitate the documentation of accountability and compliance
- Require completion of a DPIA with every material change in how high-risk personal data is treated or processed
- Review and update our data protection supplier security assessment review ("SAR") questionnaire to include expanded personal data classifications and new protection program requirements

3. **Personnel Confidentiality Commitments & Data Protection Training**

- Staff must regularly (not less than annually) complete general data protection awareness training. We have supplemented this general training with GDPR-specific and role-specific training
- Ongoing data protection awareness communications on a variety of topics including phishing, information security, and privacy
- All employees must sign confidentiality agreements that survive the employment relationship

4. **Contract Commitments and Data Processing Agreements:** We have drafted GDPR-ready data processing addenda (DPAs) and updated our contractual language to reflect the additional accountability and compliance requirements, which primarily includes points as follows:

- Processing personal data only as instructed in writing
- Delineation of appropriate security measures
- Only engage vendors or sub-processors as generally or specifically authorized by data controller, which are contractually required to follow the same data protection obligations as data processor
- Assist data controller with responding to data subject rights' requests
- Assist data controller with implementing DPIAs and security measures
- Immediately inform data controller if any instructions from data controller are in breach of GDPR
- Return or delete data at end of contract subject to legal requirements
- Provide information that is necessary for the data controller to demonstrate compliance
- Assist data controller with breach investigation and notification

5. **Managing Our Vendors:** We have a robust vendor data protection risk assessment framework and agreement in place (i.e., Vendor Data Protection Risk Management and Procurement Processes). ICF uses vendors (e.g., Amazon Web Services, etc.) to help us provide our services or tools to our clients. Where this requires access to our clients' or their customers' personal data, ICF is responsible for the data protection practices of our vendors.

   As part of our GDPE program, we are closely connecting the privacy by design and default ('PbDs') approach with the existing Vendor Data Protection Risk Management and Procurement Processes. This results in the following key controls:

- Robust contracts that incorporate Data Protection Addenda with third parties imposing materially equivalent provisions that we have in place with our clients
- EU-approved "model clause" standard contractual agreements (Model Clauses) and/or GDPR Addendum exist to enable lawful data transfers to our vendors
- Documented Vendor Risk Data Protection Management policy and framework exist
- New vendors with access to personal data must complete a data protection SAR Questionnaire
- Vendors with access to ICF- managed systems are required to follow ICF-internal access control and identity and authorization policies, to include account reviews as appropriate
- Vendors must access ICF resources through approved mechanisms (e.g., VPN)
- Vendors have restricted access controls on traffic, users, and assets

6. **Data transfers:** We will use our multi-layered and redundant approach to cross border data transfer compliance and ensure proper safeguards are in place for personal data. This includes regionalization and EU Standard Contractual Clauses (SCCs):

- **Regional hosting:** We leverage a regional hosting strategy with many of our services hosted in the EEA and other data planned to be moved to regional hosting solutions. While the GDPR does not require regional storage and we do not think that data localization leads to better data privacy or security, we understand that many EEA clients prefer their data to be stored in the EEA. It is important to understand that while we may store clients' personal data in these data centers for certain services for some EEA clients, access to this data from outside the EEA may be required to provide the services and tools, e.g., for 24/7-support. Such data transfers are allowed thanks to the mentioned SCCs
- **SCCs:** We use model clauses that allow us to compliantly transfer personal data outside the EEA within ICF's group of companies.
- **Vendors:** Robust contracts exist with vendors and partners to ensure that data transfer requirements (and other data protection obligations) are passed on to our vendors and partners.

7. **Data Protection Officer (DPO):** We also have appointed a DPO to oversee the data protection responsibilities within the organization and ensure compliance.

8. **Keep abreast of ever-evolving global data protection and ePrivacy regulations:** The data protection and ePrivacy regulatory environment remains dynamic and subject to new regulatory action. ICF stays in touch with these changes through conferences, industry associations, and our contacts within key government agencies so that we can remain in compliance and continue to be a constructive partner.

9. **Security Measures:** As a vital component of our GDPE program, our CISO leads ICF's information security governance in consultation with our DPO and Office of the General Counsel.

   We follow a defense-in-depth information security methodology and approach, where we embed security controls throughout the system architecture and service lifecycles to make sure our measures are and remain "appropriate" to the risk involved.

   In particular, we have established policy, procedure, governance, and technical requirements to manage IT security risk across the business with key security and data protection regulations, standards, and frameworks in consideration as follows:

- Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541 et seq.) as implemented by the Office of Management and Budget (OMB) in Circular A-130 and other policy documents

- National Institute of Standards and Technology (NIST)
- International Organization of Standards (ISO) 27001
- US Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA)
- US Children's Online Privacy Protection Act (COPPA)
- US State Laws (existing and emerging 50-state patchwork)
- US Government standards - FedRAMP
- PCI Data Security Standards, where applicable
- International standards (MTCS, IRAP) HHS-IRM Information Security Program Policy, the E-Government Act of 2002, HIPAA, HITRUST, and HITECH as needed all other relevant federal policies, regulation, and legislation
- Defense Federal Acquisition Regulation Supplement (DFARS) –NIST SP 800-171 as it is applied to CDI.

Staff Controls.

ICF staff must:

- Understand defined data classifications to protect each data type
- Understand their responsibility to protect personal data
- Acknowledge and comply with policies to protect personal and sensitive information
- Undergo annual data security training
- Engage in phishing and similar test exercises
- Review data security awareness bulletins

Technical Controls:

- Maintain Security Essentials certification, SSAE 16 SOC 2 independent review, and ISO 27001 Certification for core corporate systems
- Design data centers to host mission-critical computer systems with fully redundant subsystems and compartmentalized security zones
- Core information systems reside in a commercial grade data center with climate controls, fire suppression, redundant power, and several telecommunication options
- Computing infrastructures protection by multiple independent layers of security measures
- Grant protected network access based on the principle of least privilege

- Utilize appropriate authentication methods such as multifactor (two factor) to control access by remote users
- Email gateways check messages for possible viruses or threats
- Control workstations and servers through a central management system
- Utilize systems to securely encrypt and transfer files with sensitive data at rest and in transit
- Utilize systems that provide the capability to send and receive information with comprehensive file tracking and reporting
- Apply encryption algorithms that comply with best practice implementations. ICF has several forms of encryption. As a standard, laptops are fully encrypted using commercial grade encryption. Advanced Encryption Algorithm (AES) is another encryption algorithm used when individual file encryption is required, such as for documents and spreadsheets
- Advanced next generation firewalls and automated intrusion detection and prevention systems are in place at the network perimeters to prevent denial of service attacks, network scanning, and exposer of internal information systems and other potential threats
- Conduct routine security scans and assessments (e.g., vulnerability, pen testing, access account reviews, etc.) and review vulnerabilities and emerging threats
- Configure vulnerabilities scans to scan information systems on a regular basis using best of breed security software
- Apply prompt security updates through frequent patch management processes
- External systems reside in a DMZ or equivalent networks separation and no external Internet traffic is allowed directly into the internal production network
- Centralized configuration management for patch management, antivirus/malware protection, software distribution, operating system deployment, network access protection, and hardware and software inventory

10. **Security Incident Management Process – Incident Response and Remediation Controls:** Our Corporate Information Security Office, in collaboration with our Data Protection Team, establishes and implements our incident management plan to facilitate a quick, effective, and orderly response to all data protection incidents. Such incidents can involve:

- Information system failures and service loss
- Denial of service, intrusions, or attempted intrusions
- Viral contamination
- Breaches of confidentiality
- Security weaknesses in, or threats to, systems or services
- Lost or stolen equipment

ICF's incident response process includes, but is not limited to:

- An online procedure to facilitate swift identification and investigation; properly collecting and sufficiently protecting evidence
- Remediation procedures in case of an incident
- An escalation procedure for reporting to upper management
- Communication plan among the technology staff and decision makers within ICF

11. **Breach notification:** For most of our products and services, ICF is a data processor under GDPR and GDPR-like regimes. The obligation to notify data protection authorities and individuals in case of a breach that involves ICF would therefore lie with our clients. However, the GDPR requires data processors such as ICF to notify their clients (data controllers) without undue delay (i.e., "promptly") in such a case.

    We have the below measures in place that support our clients meeting their obligations in the event of a personal data breach at ICF related to a client:

- Facilitates swift identification, investigation, and remediation in case of an incident
- Allows for prompt notifications to clients
- Antivirus software is installed on all computers and updated on a regular basis

ICF is committed to complying with the GDPR and all data protection regulations, even as they evolve over time. ICF keeps abreast of data protection regulatory changes to provide our clients with the protection – and peace of mind – they deserve.

Many other companies are taking similar steps. The ePrivacy and data protection regulatory environment remains dynamic and subject to new regulatory action. ICF stays in touch with these changes through conferences, industry associations, and our contacts within key government agencies so that we can remain in compliance and continue to be a constructive partner.

How ICF's GDPR and similar data protection compliance implementation supports our data subjects and clients

Visit us at **icf.com/dataprotection**

About ICF

ICF (NASDAQ:ICFI) is a global consulting and digital services company with over 7,000 full- and part-time employees, but we are not your typical consultants. At ICF, business analysts and policy specialists work together with digital strategists, data scientists and creatives. We combine unmatched industry expertise with cutting-edge engagement capabilities to help organizations solve their most complex challenges. Since 1969, public and private sector clients have worked with ICF to navigate change and shape the future. Learn more at **icf.com**.

Any views or opinions expressed in this white paper are solely those of the author(s) and do not necessarily represent those of ICF. This white paper is provided for informational purposes only and the contents are subject to change without notice. No contractual obligations are formed directly or indirectly by this document. ICF MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Information outlined in this document should not be construed as legal advice.

ICF