ICF White Paper

Data Protection: Protecting your Data

Nov. 28, 2022

Introduction

ICF believes that a strong business reputation depends on a robust data protection and information security framework. We view data protection and information security as fundamental components of doing business. We are committed to protecting information assets, personal data, and client information.

The purpose of this document is to summarize our approach to data protection and information security. It provides an overview of how we secure client data and our information systems that support it. The specifics of these measures may vary depending on the services performed and applicable country regulatory requirements. Our data protection and information security practices are focused on sharing information appropriately and lawfully, while preserving confidentiality, integrity, and availability.

Our data protection framework

We have developed a comprehensive data protection program with consistent global privacy standards to ensure we meet our obligations across the countries and regions where we operate. Our policies and procedures are built on a strong foundation of internationally accepted privacy principles of transparency, accountability, and individual rights. We seek to continuously improve and enhance our framework and carry on our tradition of upholding high standards in collecting and processing personal data across our business practices and services.

Key aspects of our data protection framework

We have established a suite of data protection policies and procedures to meet the requirements and standards of applicable data protection laws, including:

Data protection

Our accountability and governance measures ensure that we understand and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.

Data incident management

Our data security procedures ensure that we have safeguards and measures in place to identify, assess, investigate, and report any personal data breach in line with regulatory expectations. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

Data Retention

Our retention policy and schedule ensure that we meet the ‘data minimization’ and ‘storage limitation’ principles and that personal data is stored, archived, and destroyed compliantly and ethically. We have dedicated procedures in place to meet the data subject’s rights and are aware of when data subject’s rights apply, along with any exemptions, response timeframes, and notification responsibilities.

International data transfers

We leverage a local hosting strategy as clients may prefer their data to be hosted within a specific jurisdiction, whether that is in the US, EEA, or UK. However, for certain services the provision of 24/7 support may require data to be stored in centralized locations across borders. Where this is the case, we have taken steps to guarantee the correct safeguards are in place to allow for data transfers and ensure we meet the compliance obligations set out in applicable local law. For example, where appropriate, EU-approved Standard Contractual Clauses are incorporated within our client and supplier contracts to extend GDPR rights and safeguards accordingly.

Where ICF stores or transfers personal data outside the EU, we have appropriate procedures and additional safeguarding measures in place to also secure, encrypt and maintain the integrity of the data.

Training and awareness

We have a mandated employee training program that is provided to all employees upon hire and annually thereafter. Ongoing privacy awareness communications and activities are conducted often, and specialized training sessions are provided for specific roles or departments as appropriate.

Record keeping

We maintain records of our processing activities, ensuring that our obligations under applicable laws, including Article 30 of the GDPR, are met.

Privacy notices

We provide privacy notices to individuals to inform them why we need their personal data, how it is used, what their rights are, to whom the information is disclosed, and what safeguarding measures are in place to protect their information.

Consent

We have mechanisms for obtaining and recording consent, making sure that we can evidence an affirmative opt-in and an easy way to withdraw consent at any time.

Data protection impact assessments (DPIA)

We have developed procedures and templates for carrying out privacy impact assessments that comply with the GDPR's Article 35 requirements. We have processes in place to assess risk when we process personal data that is considered high risk, involves large-scale processing, and/or includes special category data.

Processor agreements

Where we use any third party to process personal data on our behalf (for example, research services), we have drafted compliant processor agreements and due diligence procedures for ensuring that they (as well as we) meet and understand their/our data protection obligations.

Information security, technical and organizational measures

ICF takes the privacy and security of personal data very seriously and has implemented administrative, physical, and technical safeguards to protect and secure the personal data that we process. Our Chief Information Security Officer leads our Information Security Governance in consultation with our Data Protection Officer and Office of General Counsel.

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

We have established policy, procedure, governance, and technical requirements where applicable 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 SO-state patchwork)
- US Government standards – FedRAMP
- PCI Data Security Standards,
- International standards (MTCS, IRAP) HHS-IRM Information Security Program Policy, the E-Government Act of 2002, HIPAA, HITRUST, HITECH, and, 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.

Technical measures include, but are not limited to:

- Desktop and laptop full disk encryption
- Encryption of data in transit
- Removable media encryption tools
- Desktop and laptop firewalls
- Antivirus and anti-malware software
- Multifactor authentication approaches

- Automated patching and security vulnerability assessments
- Strong physical, environmental, network, and perimeter controls
- Intrusion detection and prevention technologies
- Monitoring and detection systems

Information Security Audits

To provide us with a more complete view of our information security compliance, our services and data centers are subject to audits. We conduct several forms of audit:

- Independent third-party compliance audits against ISO 27001:2013 to certify the Information Security Management System employed within our global data centers and core corporate systems
- Annual SOC 2, Type 2 attestation and Hi-Trust report conducted by an independent third-party auditor, which encompasses the security, confidentiality, and availability principles
- Cyber Essentials Plus certification for core corporate systems and operations in the UK and Belgium
- Network vulnerability scans, which focus on the technical aspects of our Global Information Security Policy, such as patch management, application security, and infrastructure security

Data Privacy team

ICF has a full-time, dedicated data privacy team to oversee our privacy program and ensure its continued success. The 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 remain in compliance and continue to be a constructive partner.

If you require further information regarding our data protection framework, you can contact the Data Privacy team by emailing dataprotection@icf.com.

In Summary

ICF secures the information assets of our clients by adhering to a global data protection and information security framework.

Our global applications and systems are subject to both data privacy impact assessments and security certification reviews, which support a robust, consistent approach in deployment and operation.

We protect personal data within our network using appropriate physical, technical, and organizational security measures.

We confirm that our contracts with third-party processors contain provisions that are commensurate with our own policies, practices, and controls to confirm that your data is managed properly and securely in accordance with legal and regulatory requirements.

Clients and individuals rightfully demand accountability from any organization handling their personal and confidential data. We understand the importance of taking appropriate steps to safeguard information assets and are committed to protecting your data. If you have any questions or require further information on how we protect you and your business, please contact your ICF representative.