How iCIMS Supports Your Readiness for the European Union General Data Protection Regulation

The GDPR is the EU’s next generation of data protection law. Aiming to strengthen the security and protection of personal data, the GDPR replaces the 1995 European Union Data Protection Directive. Companies like iCIMS that value data security and privacy invest in being GDPR ready.

Who is Impacted by the GDPR?

The GDPR applies to organizations headquartered within the EU and organizations headquartered outside of the EU that offer goods or services to EU businesses. In our technology-driven world, this regulation impacts many global organizations.
What New Requirements Does the GDPR Have?

The GDPR builds upon existing EU data protection law, but is different from the 1995 EU Privacy Directive that was based on fundamental principles and evolving guidance. GDPR takes a more extensive approach with 99 different articles and many sub articles. Regulations this comprehensive have never existed in the world of privacy before as these new regulations govern virtually every aspect of an organizations’ handling of personal data.

The 99 Articles of the GDPR are as follows:

- General Provisions (1-4)
- Principles (5-11)
- Rights of the Data Subject (12–23) including:
  - Notice and consent to use data
  - Data access rights
  - Correction and rectification of data
  - Portability of data
  - Right to be forgotten
- Controller and Processor (24-43)
- Transfer of Personal Data to Third Countries or International Organizations (44-50)
- Independent Supervisory Authorities (51-59)
- Cooperation and Consistency (60-76)
- Remedies, Liability and Penalties (77-84)
- Provisions Relating to Specific Processing Situations (85-91)
- Delegated Acts and Implementing Acts (92-93)
- Final Provisions (94-99)

Some of the highlights within both new and enhanced requirements include:

- Direct regulation of data processors
- Data security obligations
- Data governance requirements, including policies, procedures and defined roles
- Requirements for data protection by design and default, and the conduct of data protection impact assessments
- Strict data breach notification timelines (generally 72 hours)
- A data protection officer for "large scale processing" of certain data
- Individual rights for data subjects, including:
  - Notice and consent to data use
  - Data access rights
  - Correction and rectification of data
  - Portability of data
  - Right to erasure of personal data

The new regulation also comes with new penalties for non-compliance. Penalties can be triggered by one individual complaint and may be as high as four percent of global turnover or 20 million Euros (approx. $22.8 million USD), whichever is greater. Penalties may also include reprimands, bans, certification withdrawals or the imposition of a supervisory organization.
How is iCIMS Prepared for the GDPR?

iCIMS is committed to complying with the GDPR and supporting its global customer base. This includes a company-wide initiative to ensure that iCIMS satisfies internal GDPR requirements while also supporting its customers’ compliance.

Processes & Policies
iCIMS has invested in information and data protection since its inception and its GDPR compliance plan was built on this solid foundation.

Examples of compliance investments include:

ISO Certification:
According to the GDPR, approved certification methods may be used as an element to demonstrate compliance. iCIMS annually tests and maintains an ISO/IEC 27001:2013 certification that broadly covers the production and operation environments for its talent platform.

EU Privacy Shield:
iCIMS has completed the EU-U.S. Privacy Shield Certification by the U.S. Department of Commerce. Participation in the Privacy Shield program facilitates the transfer of personal data from the EU to the U.S.

iCIMS Information Security Policies:
iCIMS maintains detailed and comprehensive policies that apply to many of the areas covered by the GDPR including:

Policies Included:
- Data Security and Privacy Policy
- Incident Response Policy and Procedure
- IT Security Policy
- Talent Platform Security Policy
- Comprehensive internal policies and process controls

Areas Covered:
- Use of information
- Comprehensive information security
- Data handling
- Certified data centers
- Incident response
- Training and monitoring
Readiness Program

Building off this strong foundation, iCIMS had a comprehensive program across its entire operation to ensure that it was GDPR-ready.

To address the complexity and risks of becoming GDPR-ready, iCIMS used a multi-level approach that pools the knowledge of legal and regulatory counsel, consultants, and industry leaders while benchmarking its processes to globally accepted standards.

Within the readiness program, iCIMS developed a GDPR Compliance Framework which focuses on three groups:

1. Legal and Regulatory
2. Organizational
3. Technical

Within these buckets, iCIMS is covering key areas, including, but not limited to:

- Data Subject Rights
- Data Subject Consent
- Defining Roles and Responsibilities
- Embedding Privacy into and across all of the organizational and technical areas of the platform and corporate operations

As part of iCIMS’ commitment to complying with the GDPR, iCIMS’ team of experts have worked through a detailed remediation program. iCIMS has completed analysis of every aspect of its company that touches personal data, including:

- The iCIMS Talent Platform
- Corporate infrastructure
- Company processes
- iCIMS’ systems
How Can My Organization Be GDPR Ready?

iCIMS understands that businesses today work with a variety of vendors. To ensure GDPR compliance, organizations should make sure their vendors have the know-how, experience and commitment to support the kinds of comprehensive measures that the GDPR requires.

Data security and compliance are a top priority for iCIMS as a best-of-breed recruitment technology provider. As iCIMS’ existing data privacy and protection infrastructure demonstrates, iCIMS has the history, skills and commitment to continue to work diligently to create a secure, seamless user experience for iCIMS’ customers in the U.S., EU and around the world.

iCIMS is committed to maintaining GDPR compliance and enabling its customers to use the iCIMS Talent Platform to assist in their own GDPR compliance. As so, we’ve put together the following resources to help our customers become and remain GDPR compliant.

Understanding How the iCIMS Talent Platform Can Support GDPR Compliance
General Data Protection Rights 2018 video
Guide for iCIMS Talent Platform Customers to Certain GDPR Compliance Functions
Getting Ready for GDPR Using Existing Platform Capabilities
Preparing for the GDPR Outside of the EU
An Introduction to the GDPR for Human Resource Professionals
Guidelines on Consent Under the GDPR
Trading Privacy for Convenience: The Dilemma Facing Today’s Job Candidates

Visit gdpr-info.eu for more information on the GDPR and other EU data protection developments.

About iCIMS: iCIMS is the leading provider of talent acquisition solutions that help businesses win the war for top talent. iCIMS empowers companies to manage their entire hiring process within the industry’s most robust Platform-as-a-Service (PaaS). Built on the foundation of a best-to-market talent acquisition software suite, iCIMS’ PaaS framework, UNIFi, allows employers to expand the capabilities of their core talent acquisition technology by integrating with the largest partner ecosystem in talent acquisition to help them attract, find, screen, and manage candidates. Offering scalable, easy-to-use solutions that are backed by award-winning customer service, iCIMS supports more than 3,500 contracted customers and is one of the largest and fastest-growing talent acquisition solution providers.