KORN FERRY
Executive Search | HayGroup | Futurestep

GDPR Update Statement

Introduction

On May 25, 2018, the European Union's (EU) General Data Protection Regulation (GDPR or Regulation) goes into effect. The GDPR is a significant change for global data privacy law and introduces complex rules for organizations involved in the collection and processing of personal data of individuals located in the EU. The new Regulation:

- updates, strengthens, unifies, and clarifies existing EU data protection law;
- gives individuals in the EU more consistent rights to access and control their personal data; and
- requires the implementation of enhanced policies and procedures by businesses that process personal data of EU individuals.

Our Commitment

As the preeminent global people and organizational advisory firm, Korn Ferry takes its responsibility to protect personal data very seriously.

Trust is the cornerstone of our relationships with clients, individuals, and the public. We're committed to the security and protection of the personal data that we collect, and we constantly strive to provide a compliant and consistent approach to data protection.

Korn Ferry continuously evolves its security and privacy programs to develop effective programs that demonstrate an understanding of, and an appreciation for, applicable laws including the new Regulation.

This statement summarizes our preparation and objectives for GDPR compliance.

How We're Preparing for the GDPR

Complying with the GDPR requires organizations to rethink the way that business is done. For Korn Ferry, this includes updating our data collection, use, transfer, disclosure, and disposal policies and procedures. Our preparation includes:

- ***Global Privacy Policy*** – We're updating our Global Privacy Policy for the GDPR, so that individuals whose personal data we process can be informed of why we need it, how it's used, what their rights are, to whom the information is disclosed, and what safeguarding measures are in place to protect their information.

- ***Data Retention*** – We're updating our data retention policy and schedule in light of the GDPR *'data minimization'* and *'storage limitation'* principles, which govern how personal data is stored, archived, and destroyed.

- ***Data Breaches*** – We're updating our data breach response procedures to help us discover, contain, and remediate data security incidents as well as providing required notices to individuals and EU Data Protection Authorities.

- ***International Data Transfers & Third-Party Disclosures*** – Where Korn Ferry stores or transfers personal data outside the EU, we have procedures and safeguarding measures in place to assist us in securing, encrypting, and maintaining the integrity of the data. On a corporate level, Korn Ferry has entered into Inter-Affiliate Data Transfer Agreements. When engaging subcontractors, including hosting providers, Korn Ferry

carries out due diligence checks and ensures that appropriate protections are in place. Korn Ferry also enters into the EU Standard Contractual Clauses at client request.

- ***Data Subject Rights (DSR)*** – Korn Ferry is improving its internal policies and procedures, and developing new procedures as needed, so we can respond appropriately to individual rights requests. We have updated our DSR procedures to accommodate the GDPR one-month timeframe for responding to the requests.

- ***Legal Basis for Processing*** - We're reviewing all processing activities to identify the relevant legal basis. Where applicable, we also maintain records of our processing activities, in order to meet our obligations under Article 30 of the GDPR. In part, we are identifying and assessing what personal data we hold, where it comes from, how and why it is processed, and if and to whom it is disclosed.

- ***Obtaining Consent*** – Where consent is an appropriate legal basis, we are revising our consent mechanisms for obtaining personal data, to help individuals understand what they are providing, why and how we use it, and how to provide consent to our processing of their information. We have in place processes for recording consent, along with time and date records.

- ***Direct Marketing*** – We are updating our wording and processes for direct marketing, including notice, opt-in and opt-out mechanisms, and unsubscribe features on our marketing materials.

- ***Third Party Risk Management*** – We're building on our existing risk assessment processes and evaluating our current and new third-party service providers with an eye to GDPR compliance. This includes updating contracts with our service providers that process personal data on our behalf. We've developed due diligence procedures to help these third parties understand and meet their obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the third party's technical and organizational measures in place, and their compliance with the GDPR.

Information Security & Technical and Organizational Measures

Korn Ferry recognizes that personal data is only as secure as the tools and technologies that manage it. We take appropriate measures and precautions to protect and secure personal data that we process. We have information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure, or destruction. Our corporate systems have several layers of security measures, including:

- ***Security Organization*** – Korn Ferry has implemented a series of information technology security and data protection policies and programs, managed and enforced by Korn Ferry's Chief Information Security Officer and global security organization, who report to the Chief Information Officer and work in tandem with the Privacy team. Korn Ferry manages security programs in accordance with our Information Technology Security Policies and Procedures (IT Security Policy), designed and administered following the guidelines set forth in ISO 27001. Korn Ferry executive management regularly reviews and approves the policies and associated procedures. Korn Ferry conducts ongoing reviews and assessments of our security and data privacy programs and of our infrastructure. Continuous improvement of Korn Ferry's security posture has enabled us to address data protection challenges on a global and diverse industry basis.

- ***Data Center, Network & Systems Protection*** – Korn Ferry systems reside in Tier III or greater SSAE 16 certified hosting facilities with security measures, protections and controls commensurate with their rating designation. Korn Ferry servers are protected by perimeter firewalls, and most are protected with network intrusion detection and prevention systems. As required by our IT Security Policy, Korn Ferry servers and workstations run anti-virus software with proactive threat protection.

- ***Email, Remote Access, Application Security Scanning*** – Korn Ferry's internal network is also protected with email and web security scanning. Korn Ferry's remote access solution is a virtual private network (VPN) that utilizes a 256-bit encrypted link. Applications are developed with the latest secure coding techniques such as SQL injection and cross-site scripting to protect against malicious exploits and undergo application security scanning using an outside service on a regular basis.

- ***Network Vulnerability Scanning*** – Korn Ferry regularly performs vulnerability scans of our entire infrastructure including internal and external facing servers. Vulnerabilities are tracked and managed according to our vulnerability management policy, which requires remediation according to a schedule based on severity of the vulnerability. This effort is supported by an active patch management program.

- ***Security Monitoring & Incident Response Plan*** – Korn Ferry's infrastructure is also monitored by its Security Incident Event Monitoring solution which correlates logs from perimeter devices (firewalls, intrusion detection system/intrusion prevention systems, routers and other equipment) as well as security devices and software (antivirus, domain controllers, RSA servers and others). These monitoring solutions alert us automatically when unexpected activity or activity levels occur. Korn Ferry also maintains a formal Incident Response Plan and disaster preparedness.

- ***Access Control*** – Korn Ferry has an access control policy that includes least privileged and role-based access restrictions applied to all resources and information with unique IDs for each individual to include strong passwords with complexity, length and aging requirements. We use Transport Layer Security (TLS) web session security. A bonded carrier service with an unbroken chain of custody transports backup tapes to the offsite storage location. Remote access and access to server management functions require administrative privileges and multi-factor authentication. Critical servers also have special single-use passwords enabled.

- ***User Training, IT Security Policy, Code of Business Conduct & Physical Record Policy*** – All Korn Ferry employees are required to agree to the Korn Ferry Code of Business Conduct and Ethics and IT Security Policy as a condition of employment and as appropriate thereafter. Korn Ferry's current practice requires new employees to pass a background check at the time of hire, as permitted by applicable law and in accordance with Korn Ferry's policies and local practices. This background check may include a check of criminal history, employment history, sanctions check and education verification. We have established a clean desk policy, locked files, and other physical access controls, including electronic fob or access cards.

- ***Encryption in Transit*** – Korn Ferry encrypts e-mail data in transit using the TLS 1.2 protocol when communicating with a server that accepts encrypted connections. Sensitive documents attached to e-mail can be encrypted and password protected. Data and information exchange is further enforced by our Data Loss Prevention solution. Clients can also use Korn Ferry's Secure File Transfer System (SFTS). The SFTS is

accessed only by authorized personnel via a secure link with encryption in transit and at rest.

- ***Encryption for Internal Korn Ferry networks*** – Network systems make use of encryption, session controls, routing tables and access control lists (ACLs) to ensure that communications follow approved paths with appropriate protections enabled.
- ***Encryption at Rest*** – Most information received by Korn Ferry via e-mail or SFTS is encrypted at rest on its servers. Where supported by the Korn Ferry services, data collected by Korn Ferry through client's use of the contracted services is encrypted at rest on Korn Ferry servers and backup media.
- ***Change Management*** – Korn Ferry follows an Information Technology Infrastructure Library (ITL) based framework and well-defined change management process on all production systems and applications. Significant and major changes are discussed and voted on by a Change Advisory Board.
- ***Application Release Management*** – Korn Ferry uses non-production systems for the development, testing and staging of Korn Ferry developed applications. Only when the application release has been tested, including application security scanning and QA review, will it be migrated to the production system, pursuant to our change management process.

Moving beyond May 2018, we are working to achieve ISO 27001/27018 certification for key technology platforms and processes to demonstrate a globally recognized validation of the maturity of our global privacy and security programs.

GDPR Roles and Employees

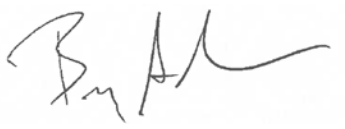
Korn Ferry's Privacy Executive Committee has appointed a privacy team to develop and implement our roadmap for complying with the new Regulation. This team is responsible for promoting awareness of the GDPR across the organization, assessing our GDPR readiness, identifying and addressing any gap areas, and implementing the new policies, procedures and measures discussed here.

Although privacy and confidentiality are embedded in our global standards, methodologies, training and practice, we understand that the requirements of the GPDR are complex. We recognize that employee awareness and understanding is vital to continued compliance. We are updating our privacy training programs to educate our employees on how to handle personal data under the GDPR and other privacy laws.

If you have any questions about our preparation for the GDPR, please contact us at privacy@kornferry.com or, if by postal mail, at Korn/Ferry International; 1900 Avenue of the Stars, Suite 2600; Los Angeles, CA 90067, U.S.A., Attn: Privacy Office.

Date: 17 May 2018

Jonathan M. Kuai
General Counsel and Co-Chief Privacy Officer



Bryan Ackermann
Chief Information Officer and Co-Chief Privacy Officer