KORN FERRY®

GDPR and Data Protection Measures

Introduction

The European Union's (EU) General Data Protection Regulation ("GDPR" or the "Regulation") went into effect on May 25, 2018. It was a significant change for global data privacy law and introduced complex rules for organizations involved in the collection and processing of personal data of individuals located in the EU. The Regulation:

- Updated the previous EU privacy framework to create a common set of data privacy and security rules across the EU.
- Reinforces principles of transparency and openness with individuals as to what data companies hold about them and how it is used.
- Provides individuals in the EU more consistent rights to access and control their personal data.
- Establishes a general accountability requirement, requiring companies to be able to demonstrate the ways in which they comply with data protection principles.

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 have always been committed to the security and protection of personal data and we constantly strive to provide a compliant and consistent approach to data protection.

Korn Ferry's security and privacy programs are continuously evolving, demonstrating an understanding of and an appreciation for applicable laws, including in anticipation of new and future regulations.

This statement summarizes our preparation and objectives for compliance with applicable privacy laws, including the GDPR.

How We Prepared for the GDPR and Our Continued Efforts

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

- ***Global Privacy Policy*** – Our Global Privacy Policy has been updated for the GDPR so that individuals whose personal data we process are informed of what data we collect, why the data is required, how it is used, what their rights are, to whom the information is disclosed, and what safeguards are in place to protect their information.
- ***Data Retention*** – Our Data Retention Policy has been updated and we are in the process of updating the data retention schedule, to reflect the GDPR *'data minimization'*

and *'storage limitation'* principles, which govern how personal data is stored, archived, and destroyed.

- ***Data Breaches*** – Our data breach response procedures were updated to help us discover, contain, and remediate data privacy and security incidents. This included the required notice provision to individuals and relevant supervisory authorities.
- ***International Data Transfers & Third-Party Disclosures*** – We enhanced our procedures and safeguarding measures to secure, encrypt, and maintain data integrity during the transfer and/or storage of personal data outside the EU. On a corporate level, Korn Ferry has entered into Interaffiliate Data Processing and Transfer Agreements. When engaging subprocessors, including hosting providers, Korn Ferry carries out due diligence and vetting processes to ensure that appropriate protections are in place. Korn Ferry also adopts the EU Standard Contractual Clauses at client request.
- ***Data Subject Rights*** – We improved our internal policies and procedures and developed processes to respond to data subject requests within the legally-prescribed timeframe.
- ***Legal Basis for Processing*** – We review all processing activities to identify the relevant legal basis. Where applicable, we 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 and Providing Notice*** – We have revised our consent and notice process to help individuals easily understand what personal information is being collected, how it will be used and for what purpose. We articulate the individual's rights to access and control their personal data.
- ***Direct Marketing*** – We have updated our wording and processes for direct marketing, to include notice, opt-in and opt-out mechanisms, and unsubscribe features on our marketing materials.
- ***Third Party Risk Management*** – We updated our existing risk assessment processes and continue to evaluate our current and new third-party service providers. This includes updating contracts with our service providers that process personal data on our behalf. We 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.
- ***ISO/IEC 27001 and ISO/IEC 27018 Certifications*** – The International Organization for Standardization (ISO) is an independent nongovernmental organization that develops and publishes voluntary international standards. Korn Ferry has been certified by the British Standards Institute (BSI) to ISO/IEC 27001 and ISO/IEC 27018 under certificate numbers IS 700177 and PII 707431, respectively, for key platforms and processes. ISO/IEC 27001 is the international standard that describes the specifications for establishing, implementing, maintaining and continually improving an information security management system. ISO/IEC 27018 is a code of practice for protection of personally identifiable information in public clouds. It establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information in accordance with privacy principles. It builds upon the ISO/IEC 27001 framework. Korn Ferry's certifications evidence our commitment to

best practice information security methods, compliance with globally recognized standards, and demonstrate the maturity of our global privacy and security programs.

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 technical and organizational 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 its Information Technology Security Policies and Procedures, which were designed and administered following the guidelines set forth in ISO 27001. Korn Ferry's executive management and security teams regularly review policies and procedures and conduct assessments of its security and privacy programs. Continuous improvement of our 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 which commensurate with their rating designation. Korn Ferry's environment is protected by perimeter firewalls and technology including network intrusion prevention/detection systems and anti-virus software with proactive threat protection.

- ***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.

- ***Email, Remote Access, Application Security Scanning*** – Korn Ferry protects its email and web with security scanning. A 256-bit encrypted link is deployed for its virtual private network (VPN) remote access solution. Applications are developed with the latest secure coding techniques to protect against malicious exploits such as SQL injection and cross-site scripting. Vulnerability, penetration and security scanning is regularly done using an outside service as a proactive measure.

- ***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 prevention/detection systems, routers and other equipment) as well as security devices and software (antivirus, domain controllers, MFA servers and others). These monitoring solutions alert us automatically when unexpected activity 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 transports backups, archives, and other media to offsite storage locations. Remote access and access to server management functions require administrative privileges and multi-factor authentication. Critical servers also have special single-use password enablement.

- ***User Training, IT Security Policy, Code of Business Conduct and Physical Record Policy*** – Korn Ferry employees participate in regular compliance training. All Korn Ferry employees are required to agree to the Korn Ferry Code of Business Conduct and Ethics, Agreement to Protect Confidential Information, 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. Korn Ferry has established a clean desk policy, locked files, and other physical access controls, including electronic fob and access cards.

- ***Encryption in Transit*** – Korn Ferry encrypts email data in transit using the TLS 1.2 protocol when communicating with a server that accepts encrypted connections. Enhanced encryption techniques have been deployed to easily encrypt assessments and email files. Data and information protection 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*** – Where supported by the Korn Ferry services, data received by Korn Ferry via email, SFTS or 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 (ITIL) based framework and a well-defined change management process on all production systems and applications. Significant and major changes are reviewed and controlled by the associated management.

- ***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, will it be migrated to the production system pursuant to our change management process. Production data is stored only in production systems or systems with production-level controls.

GDPR Roles and Employees

Korn Ferry's Privacy Executive Committee appointed a Privacy team to develop and implement a roadmap for complying with the GDPR and other data privacy laws. This team is responsible for promoting awareness of privacy 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 continually updating and monitoring our privacy training programs to ensure we are educating our employees on how to handle personal data under the GDPR and other privacy laws.

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

Date: 24 October 2019

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

Brandon Johnson
Chief Information Officer and Co-Chief Privacy Officer