KORN FERRY

Data Protection Measures

Our Commitment

As a leading global organizational consulting firm, Korn Ferry works with our clients to design optimal organization structures, roles, and responsibilities. We help them hire the right people, focus on the right skills, and advise them on how to reward, engage, and motivate their workforce while developing professionals as they navigate and advance their careers.

Trust is the cornerstone of our relationships with clients, individuals, and the public. We strive to provide a compliant and consistent approach to data protection. Taking a holistic approach to privacy and security, Korn Ferry aims to regularly evolve its information security and data privacy programs and practices. We do this to promote the safety, security, and responsible use of the information and data entrusted to us.

The Privacy and Security teams work together to design and implement policies and programs to address applicable and anticipated laws and regulations. We also work to monitor and assess ongoing threats, keep data safe from cybersecurity attacks and breaches, and maintain relevant privacy and security certifications. The Privacy and Security teams proactively partner with our Digital product teams to embed privacy and security by design principles into product development and operations. Information security policies and procedures are in place and specifically designed to protect personal information from unauthorized access, alteration, disclosure, or destruction.

The Privacy and Security functions are governed by the Privacy Executive Committee / Security Executive Committee, which meets on a regular basis to discuss matters pertaining to data privacy and cybersecurity. The committee includes senior representatives from Korn Ferry’s IT, Security, Privacy, Legal, Finance, Digital, and Human Resources teams. The executive management, Privacy and Security teams are responsible for reviewing our security and privacy programs and policies.

This statement summarizes our preparation, objectives, and current measures for compliance with applicable privacy laws.

Privacy

The privacy landscape is continuously evolving and becoming increasingly complex. This dynamic environment demands a proactive approach to privacy management, where vigilance and adaptability are key to maintaining trust and compliance. The key principles of privacy laws are designed to protect individuals’ personal data and hold organizations accountable for ensuring this data is handled in a secure, fair and transparent manner.

Privacy Program and Data Protection Measures

Complying with frequent changes in legislation requires organizations like Korn Ferry to update existing elements of our program regularly. Korn Ferry works to keep pace with the changing data privacy landscape by regularly reviewing and updating our practices regarding how we collect, use, transfer, disclose, and dispose of data. Our measures include the following:

- ***Privacy Organization*** – Korn Ferry has an extensive data privacy program, supported by legal and operational specialists with expertise in privacy and data protection. The team reports to the Co-Chief Privacy Officers and works with internal Legal and Security teams.

  The global team is responsible for managing Korn Ferry's Personal Information Management System (PIMS), which includes policies like the Global Privacy Policy aligned with the guidelines outlined in ISO standard 27701.

  External legal counsel and other specialist consultants are engaged to support the team as required from time to time.

  The global Privacy team fosters a culture of privacy within the organization by partnering with business and corporate teams, performing collaborative risk assessments, providing awareness and training, and creating and communicating policies and guidelines on handling personal data.

- ***Global Privacy Policy*** – Korn Ferry's Global Privacy Policy (available here) is designed to address applicable data privacy laws and the full data life cycle, which includes the collection, use, retention, processing, disclosure, and destruction of information. We regularly review our Global Privacy Policy and update it to incorporate new data protection legislation requirements applicable to our services. Under our policy, individuals whose personal data we process are to be informed of what data we collect, for what purpose, 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*** – Korn Ferry has a Data Retention and Classification Policy that reflects foundational privacy principles of 'data minimization' and 'storage limitation', which govern how personal data is stored, archived, and destroyed, as well as procedures for the retention and destruction of internal and customer records and documents, electronic and otherwise.

- ***Data Breaches*** – Korn Ferry regularly tests and updates our data breach response procedures in order to detect, contain, and remediate privacy and data security incidents. The procedures include mandatory notification provisions to individuals, clients, and relevant supervisory authorities as appropriate.

- ***International Data Transfers and Third Party Disclosures*** – Korn Ferry employs safeguards to secure, encrypt, and protect data privacy during the transfer and storage of personal data. Korn Ferry relies on our Interaffiliate Data Processing and Transfer Agreement between Korn Ferry subsidiaries worldwide to transfer covered data lawfully. When engaging subprocessors and service providers, including hosting providers, Korn Ferry conducts due diligence through the Third Party Risk Management process, and completes data transfer impact assessments as needed, to determine that appropriate protections and transfer mechanisms are in place. Specifically, for the European Union's General Data Protection regulation (GDPR), Korn Ferry has adopted the latest version (as of publication of this document) of the EU Standard Contractual Clauses (see pre-signed copy for clients here) and has a process in place designed to support vendor and client compliance (see pre-signed copy for clients here). Data transfer impact assessments to facilitate transfers of personal data out of the EU are periodically completed. Also related to data transfers, we believe it is very unlikely Korn Ferry (US) is subject to FISA as we do not provide communication services to the public and we have never been issued a directive under FISA.

- ***Data Subject Rights*** – Korn Ferry has established internal policies, procedures, and processes to respond to data subject requests within legally-prescribed timeframes. See the Choices and Individuals' Rights section of our Global Privacy Policy for more information on how individuals globally can exercise their rights.

- ***Legal Basis for Processing*** – Korn Ferry has instituted a formal process to determine the relevant legal basis for our data processing activities. Where applicable, we maintain records of our processing activities to meet our obligations under Articles 30 and 35 of the GDPR, the Brazilian General Personal Data Protection Act (LGPD), and other laws. We periodically identify and assess 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*** – For relevant services, Korn Ferry utilizes the consent and notice process to help individuals easily understand what personal information is being collected, how it will be used, and for what purpose. Through this process, we also articulate how individuals can exercise their rights to access and control their personal data.
- ***Third Party Risk Management*** – Under Korn Ferry's Third Party Risk Management Program, we assess current and new third-party service providers and subprocessors regularly to determine whether they meet Korn Ferry's privacy and cybersecurity requirements. To help these third parties understand and meet their obligations, Korn Ferry uses various due diligence procedures and standardized contracts that incorporate data protection obligations. These procedures may include initial and ongoing reviews of the service provided, the necessity of the processing activity, technical and organizational measures, contractual terms, and compliance with applicable laws and regulations.
- ***Direct Marketing*** – Korn Ferry designs our communications and processes for direct marketing to include required opt-in and opt-out mechanisms.
- ***ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 27701 Certifications*** – The International Organization for Standardization (ISO) is an independent non-governmental organization that develops and publishes voluntary international standards. The British Standards Institute (BSI) certified Korn Ferry in ISO/IEC 27001, ISO/IEC 27018, and ISO/IEC 27701 under certificate numbers IS 700177, PII 707431, and PM 812731, respectively, for our key technology platforms and processes across global operations. ISO/IEC 27001 is the international standard that describes the specifications for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). ISO/IEC 27018 is a code of practice for the protection of personally identifiable information in public clouds. It establishes commonly accepted controls and guidelines for implementing measures to protect personally identifiable information in accordance with privacy principles. It builds upon the ISO/IEC 27001 framework. ISO/IEC 27701 is an international standard that defines the requirements for establishing, implementing, maintaining, and continuously improving a Personal Information Management System (PIMS) for the management and protection of personal data. Certification to these internationally recognized standards demonstrates Korn Ferry's commitment and adherence to best practice information security methods, compliance with globally recognized standards, and maintenance of mature global privacy and security programs. Korn Ferry pursues regular improvement of our practices through yearly BSI audits.

Information Security & Technical and Organizational Measures

Korn Ferry believes that the security of personal data rests on the foundation of our security program. Our program encompasses information security policies and procedures specifically designed to protect personal information from unauthorized access, alteration, disclosure, or destruction. It also includes technical and organizational measures and precautions designed to protect and secure personal data that we process. Our security systems and capabilities are mutually supporting and include:

- ***Security Organization*** – Korn Ferry has an extensive global security program that is managed and enforced by Korn Ferry's Vice President of Security and the global security organization. The team reports to the Senior Vice President, Chief Information Officer and regularly works with internal Product Development and Privacy teams. Third party security firms have assisted with the design and assessment of our security program.

The global security team is responsible for managing Korn Ferry's Information Security Management System (ISMS), which includes policies like the Information Technology Security Policy aligned with the guidelines outlined in ISO standards 27001 and 27018.

- ***Data Centers, Cloud Infrastructure, Network & Systems Protection*** – Korn Ferry systems reside in cloud hosting providers with SOC 2 Type II compliant data centers. Korn Ferry uses dedicated technology to assess the security of the configuration of cloud infrastructure. Korn Ferry's environment is protected by network security technologies including web application firewalls and anti-virus software with proactive threat protection. Korn Ferry's Cloud Infrastructure Board sets governance guidelines for cloud infrastructure across the enterprise, including priorities for cloud security and operational excellence, targeted security and privacy training for developers, and direction of cloud investments, such as disaster recovery for digital applications. The Cloud Infrastructure Board meets regularly and includes representatives from Korn Ferry's IT, Security, Privacy, Cloud Operations, and Digital teams.

- ***Network Vulnerability Scanning*** – Korn Ferry seeks to regularly perform vulnerability scans of our infrastructure including internal and external facing servers. Vulnerabilities are tracked and managed according to our Vulnerability Management Policy. An active patch management program supports this effort.

- ***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 injections and cross-site scripting. Vulnerability, penetration, and security scanning are done using an outside service as a proactive measure.

- ***Security Monitoring & Incident Response Plan*** – Korn Ferry's infrastructure is also monitored by its Security Information and Event Management (SIEM) 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 are designed to alert us automatically when unexpected activity occurs. Korn Ferry also maintains a formalized Security Incident Response Plan and disaster preparedness plans. Korn Ferry conducts tabletop exercises to test our ability to respond to a security incident.

- ***Access Control*** – Korn Ferry has an access control policy that includes least privileged and role-based access restrictions with unique IDs based on strong passwords with complexity, length, and aging requirements. Remote access and access to server management functions require administrative privileges, multi-factor authentication (MFA), and critical servers have special single-use password enablement.

- ***User Training, IT Security Policy, Code of Business Conduct and Ethics, and Physical Record Policy*** – Korn Ferry employees participate in regular compliance training, including monthly simulated phishing attacks. Employees with privileged access to systems participate in Security and Privacy by Design training. 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. Korn Ferry conducts pre-employment background checks in accordance with its internal policies and local practices. For its offices, 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.

This is augmented by our Data Loss Prevention solution which targets certain sensitive classes of data. Clients can also use Korn Ferry's Secure File Transfer System (SFTS) for sharing data with the Firm. The SFTS can only be accessed 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 so that communications follow approved paths with appropriate protections enabled.
- ***Encryption at Rest*** – 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 where supported.
- ***Change Management*** – Korn Ferry follows an Information Technology Infrastructure Library-based framework and a well-defined change management process on our production systems and applications. Significant and major changes are to be reviewed and controlled by our Change Approval Board, which consists of senior managers and subject matter experts.
- ***Application Release Management*** – Korn Ferry uses non-production systems for the development, testing, and staging of Korn Ferry developed applications. Once an application release has been tested, it is to be migrated to the production system pursuant to our change management process.

In Conclusion

We are committed to the security and protection of personal data, we take this responsibility seriously, and we have taken a wide range of measures to meet this commitment. We strive to embed privacy and security best practices into our global standards, methodologies, processes, and training. We recognize that employee awareness and understanding is vital to continued compliance, and our privacy and security training programs are designed to educate our employees on how to handle personal data consistent with relevant privacy laws and security best practices.

If you have any questions about Korn Ferry's privacy program, please contact us at privacy@kornferry.com or, by postal mail, at:

Korn Ferry
1900 Avenue of the Stars, Suite 1225
Los Angeles, CA 90067 U.S.A.
Attn: Privacy Office

Date: 04-12-25

Kimberly Zink

Kimberly Zink
Associate General Counsel and
Co-Chief Privacy Officer

Mike LoRusso

Mike LoRusso
Senior Vice President, Chief Information
Officer, and Co-Chief Privacy Officer