Data and Security Analyst
Washington, DC

About the Organization
ULI is a global research and education nonprofit organization whose mission is to shape the future of the built environment for transformative impact in communities worldwide. It is the oldest and largest network of cross disciplinary real estate and land experts in the world, with over 45,000 members. For more information, please visit https://uli.org.

About the Position
The Data and Security Analyst, reporting to the Sr. Vice President, Information Technology, is responsible for ensuring the safe operations of ULI's information technology environment and the secure processing, storage, and disposition of data. This position will serve as ULI's data protection officer managing data processing within ULI and with partner organizations.

Specific responsibilities include:

- Keeps current with security and data privacy laws and takes necessary steps to ensure ULI's compliance.
- Performs functions associated with a GDPR data protection officer.
- Create and maintain IT Security Incident Response Plan.
- Create and maintain registry of sensitive information that is stored across ULI and with partners. Sensitive information includes personally identifiable information (PII), financial, membership, and demographic.
- Reviews and approves contracts where ULI shares sensitive information with partner organizations.
- Reviews and approves requests to collect, store, or transfer sensitive information.
- Applies best practices securing sensitive information at rest and in transit.
- Performs regular audits to ensure sensitive information is being stored, transmitted, and disposed of properly.
- Performs regular audits of ULI's information technology environment and ensures that appropriate security measures are in place to detect and mitigate risk of attack. The information technology environment includes desktops, laptops, servers, and cloud platforms.
- Responds and investigates security alerts that are generated from security systems.
- Develop and deliver regular security training to ULI staff.
- Propose security measures that incorporate business priorities and demands.

Candidate Profile

- Bachelor's degree or equivalent work experience.
- Security or data privacy focused certifications are a plus.
- Five years of experience in information technology with at least two years of security focused experience.
- Must have a working knowledge and understanding of major global privacy regulations to include European General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and others as appropriate.

- Must have a working knowledge and understanding of NIST security frameworks to include SP800-53 Security and Privacy Controls for Information Systems and Organizations; and NISTIR-7621 Small Business Information Security.
- Must have demonstrated experience creating and maintaining a data registry of sensitive information across multiple systems, databases, and services.
- Experience with securing Azure Active Directory and managing alerts within Azure Security Center and Office 365 Security Center.
- Experience with endpoint management and device-level security.
- Strong written and verbal communication skills. Ability to explain legal and technical concepts using common language and visuals.
- Ability to balance security risk and business needs diplomatically.
- Strong ability to collaborate and develop relationships, often cross-culturally, with the ULI workforce, stakeholders, and vendors.
- Ability to develop and explain a vulnerability-probability risk matrix.

APPLICATION INSTRUCTIONS:
ULI has a robust benefits package which includes health, dental, and life insurance, vacation and a retirement plan. Compensation is commensurate with experience. Expand HR Consulting (EHR) has been retained to conduct the search. To apply, please submit your letter of interest and resume to EHR, Erica Raphael, Sr. Consultant, eraphael@expandhr.com.

ULI is proud to be an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, religion/creed, sex, national origin, disability, genetic information, pregnancy, veteran or active military status, alienage or citizenship status, arrest or conviction record, credit history, salary history, caregiver status, sexual orientation, gender identity, marital or partnership status, familial status, unemployment status, status as a victim of domestic violence, sexual violence or any other status protected by applicable law.