iapp

Privacy Engineering Domains

Physical Architect

By the 2024-2025 IAPP Privacy Engineering Section Advisory Board

"I design and manage physical spaces, ensuring that privacy is considered in every aspect of the environment. Whether it's creating private areas in office buildings or implementing physical access controls, I strive to balance functionality, aesthetics, and privacy needs to protect individuals' personal and sensitive information."

– Physical Architect

Tasks

Design privacy-compliant physical spaces: Create environments that support secure data preventing visual exposure, managing visitor access, and limiting unauthorized entry to sensitive areas like server rooms or racks.

Implement physical access controls: Use electronic locks, gates, visitor logs, biometric systems and security badges to restrict access. Closely collaborate with IT teams to ensure secure integration and data handling of biometric systems.

Assess physical spaces for privacy risks: Evaluate risks tied to physical layout, desk positioning, shared areas and specialized infrastructure, like Faraday cages for sensitive equipment.

Collaborate with IT and security teams: Align physical security — especially around infrastructure like server rooms — with digital protection strategies through close coordination with IT, security and privacy stakeholders.

Secure documentation and compliance alignment: Ensure physical environments support compliance with legal standards, such as the EU General Data Protection Regulation or Health Insurance Portability and Accountability Act, especially regarding secure access control and physical data protection.

Professional profile

Technical competencies: Knowledge of architectural design, security engineering, access control systems and physical risk management

Areas of experience: Physical security design, space planning, privacy by design principles and facilities management

Privacy tools: Use of tools like building information modeling software, surveillance planning tools, and physical access control systems

Certifications: Certified Information Systems Security Professional certification or other security-focused credentials to deepen expertise

In the organization

Reports to: Facilities management lead, chief security officer or chief privacy officer

Works with: IT security teams, protective security specialists, compliance officers, legal teams, data protection officers and facilities management

Key stakeholders: Facilities management, protective security, IT infrastructure, legal and risk management teams

Strategic drivers

Physical privacy by design: Ensure physical spaces are designed with privacy in mind, minimizing risks such as visual eavesdropping or unauthorized physical access.

Integration of privacy enhancing technologies: Use technologies such as privacy glass, sound masking systems and secure storage units.

Compliance with regulations: Design physical spaces to comply with privacy and data protection regulations, ensuring that security controls and procedures are effectively implemented.

User trust and transparency: Foster trust by providing clear information on how physical spaces are designed to protect privacy and ensure transparency in how security measures are managed.

Tools and resources

Building information modeling software: Tools like Autodesk Revit or ArchiCAD for detailed architectural designs that incorporate privacy considerations

Physical access control systems: Solutions like HID Global or Honeywell Pro-Watch for managing secure entry points and monitoring access to restricted areas

Sound masking and visual privacy technologies: Products like Cambridge Sound Management for sound masking and privacy glass solutions for visual privacy

Surveillance planning and monitoring tools: Use of CCTV planning software and integration with IT systems for continuous monitoring and incident response

Compliance management software: Tools for managing physical space compliance with privacy regulations and standards

Getting it right means

Secure and private spaces: Design includes secure meeting rooms, private workspaces and controlled access areas that prevent unauthorized viewing or access to sensitive information.

Effective access controls: The implementation of access control systems, such as key card entry, biometric authentication and surveillance systems, track and control access to restricted areas.

Compliance and risk management: There is a regularly updated documented risk management strategy and physical spaces are compliant with legal requirements.

High employee and client trust: Users of the space feel confident in the privacy and security of their environment with few to no privacy-related complaints.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

Published July 2025.

iapp.org