

Daon Data Security

Security Programs and Policies	Daon maintains and enforces a security program that addresses the management of security and the security controls Daon employs. The security program includes: • documented policies that Daon formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually; • documented, clear assignment of responsibility and authority for security program activities; • policies covering, as applicable, acceptable computer use, data classification, cryptographic controls, access control, removable media, and remote access; and • regular testing of the key controls, systems and procedures. Privacy Program. Daon maintains and enforces a privacy program and related policies that address how Personal Data is collected, used and shared.
Risk and Asset Management	Daon performs risk assessments and implements and maintains controls for risk identification, analysis, monitoring, reporting, and corrective action. Daon maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle.
Worker Education and Worker Controls	All Daon employees, agents, and contractors (collectively “Workers”) acknowledge their data security and privacy responsibilities under Daon’s policies. For Workers who Process Personal Data, Daon: • implements pre-employment background checks and screening in line with applicable legislation; • conducts security and privacy training; • implements disciplinary processes for violations of data security or privacy requirements; and • upon termination or applicable role change, promptly removes or updates Worker access rights and requires the return or destruction of Personal Data. Authentication. Daon authenticates each Worker’s identity through appropriate authentication credentials such as strong passwords, token devices, or biometrics.
Training and Awareness	Annual Security and Privacy Training. Daon’s employees complete an annual Security and Privacy awareness training on Daon’s data security, ethics and confidentiality policies and practices.

Network and Operations Management	Policies and Procedures. Daon implements policies and procedures for network and operations management. These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs, and network segregation. Vulnerability Assessments. Daon performs periodic vulnerability assessments and penetration testing on systems and applications that Process Personal Data.
Technical Access Controls	Access control. Daon implements measures to prevent data processing systems from being used by unauthorized persons, including: • user identification and authentication procedures; • ID/password security procedures (special characters, minimum length, change of password); • automatic blocking (e.g. password or timeout); and • monitoring of break-in-attempts. Data access control. Daon implements measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including: • internal policies and procedures; • control authorization schemes; • differentiated access rights (profiles, roles, actions and objects); • monitoring and logging of accesses; • reports of access; • access procedure; • change procedure; and • deletion procedure.
Physical access controls	Daon uses reputable third-party service providers to host its production infrastructure. Daon relies on these third parties to manage the physical access controls to the data center facilities that they manage. Some of the measures that Daon's service providers provide to prevent unauthorized persons from gaining physical access to the data processing systems available at premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include: • physical access control system and program in place at Daon premises; • 24x7 Global Security Operation Center monitoring physical security systems; • security video and alarm systems; • access control roles and area zones; • access control audit measures; • electronic tracking and management program for keys; • access authorizations process for employees and third parties; • door locking (electrified locks etc.); and • trained uniformed security staff. Daon reviews third-party audit reports to verify that Daon's service providers maintain appropriate physical access controls for the managed data centers.

Availability Controls	Daon implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including: • database replication; • backup procedures; • hardware redundancy; and • disaster recovery plan.
Disclosure Controls	Daon implements measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including: • logging; • transport security; and • encryption
Entry Controls	Daon implements measures to monitor whether data has been entered, changed or removed (deleted), and by whom, from data processing systems, including: • logging and reporting systems; and • audit trails and documentation.
Separation Controls	Daon implements measures to ensure that Personal Data collected for different purposes can be processed separately, including: • “least privilege” limitation of access to data by internal service; • segregation of functions (production/testing); • procedures for storage, amendment, deletion, transmission of data for different purposes; and • logical segmentation processes to manage the separation of Personal Data.
Certifications and Reports	SOC Reports. Daon maintains Service Organization Controls (“SOC”) auditing standards for service organizations issued under the AICPA. SOC 2 reports are produced annually and may be provided upon request. ISO/IEC 27001:2022 certification: Daon maintains an Information Security Management System (ISMS) which is independently audited and certified to the international standard for information security. Daon may add standards or certifications at any time.

Encryption	Daon applies data encryption mechanisms at multiple points in Daon's service to mitigate the risk of unauthorized access to Daon data at rest and in transit. Access to Daon cryptographic key materials are restricted to a limited number of authorized Daon personnel. Encryption in transit. To protect data in transit, Daon requires all inbound and outbound data connections to be encrypted using the TLS 1.2 protocol. For data traversing Daon's internal production networks, Daon uses TLS to encrypt connections between production systems. Encryption at rest. To protect data at rest, Daon leverages encryption on all server infrastructure and production data stores using industry standard encryption (AES 256).
Data Security Incident Management and Notification	Daon implements a data security incident management program that addresses how Daon manages data security incidents, including any loss, theft, misuse, or unauthorized access, disclosure, or acquisition, or destruction, or other compromise of Personal Data. In accordance with its legal obligations, Daon will notify impacted Daon users and regulatory organizations (where applicable) of validated security incidents in a timely manner.
Reviews, Audit Reports, and Security Questionnaires	Upon written request, and no more frequently than annually, Daon will complete a written data security questionnaire of reasonable scope and duration regarding Daon's business practices and data technology environment in relation to the Processing of Personal Data. Daon's responses to the security questionnaire are Daon's confidential data.
System Configuration	Daon implements measures for ensuring system configuration, including default configuration measures for internal IT and IT security governance. Daon relies on deployment automation tools to deploy infrastructure and system configuration. These automation tools leverage infrastructure configurations that are managed through code that flows through Daon's change control processes. Daon's change management processes require formal code reviews and two-party approvals prior to the release to production. Daon uses monitoring tools to monitor production infrastructure for changes from known configuration baselines.
Data Retention and Deletion	Daon implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate.