SAGE DPW

Vendor Assessment

Checklist

Table of contents

Risk Assessment and Treatment

Is there a formalized risk governance plan that defines the Enterprise Risk Management program requirements?	YES
Does the risk governance plan include risk management policies, procedures, and internal controls?	YES
Does the risk governance plan include range of assets to include: people, processes, data and technology?	YES
Is there a formalized Risk Assessment process that identifies, quantifies, and prioritizes risks based on the risk acceptance levels relevant to the organization?	YES
Is there a program to manage the treatment of identified risks?	YES
Do Subcontractors (e.g., backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, hosting providers, etc.) have access to scoped systems and data or processing facilities?	YES
Is there a documented third-party risk management program in place for the selection, oversight and risk assessment of Subcontractors (e.g. service providers, dependent service providers, sub-processors)?	YES

Does the third-party risk management program require business units to notify if there are new or changed subcontractors?	YES
Does the third-party risk management program require Confidentiality and/or Non Disclosure Agreements from Subcontractors?	YES
Does the third-party risk program require Subcontractors to notify if there are changes affecting services rendered?	YES
Does the third-party risk management program require background checks performed for Service Provider Contractors and Subcontractors?	YES
For all subcontractors requiring assessment, is there a contract?	YES
Do contracts with all subcontractors include Non-Disclosure/Confidentiality Agreements?	YES
Do contracts with all subcontractors include ownership of information, trade secrets and intellectual property?	YES
Do contracts with all subcontractors include permitted use of confidential information?	YES
Do contracts with all subcontractors include data breach notification?	YES

Do contracts with all subcontractors include Indemnification/liability?	YES
Do contracts with all subcontractors include termination/exit clause?	YES
Do contracts with all subcontractors include breach of agreement terms?	YES
Does the third party risk management program include an assigned individual or group responsible for capturing, maintaining and tracking subcontractor Information Security or other issues?	YES
Does remediation reporting include a process to identify and log subcontractor information security, privacy and/or data breach issues?	YES

Security Policy

Is there a set of information security policies that have been approved by management, published and communicated to constituents? Sage itself has an IT security department with policies employees have to follow.	YES
Have all policies been assigned to an owner responsible for review and approve periodically?	YES
Have all information security policies and standards been reviewed in the last 12 months?	YES

Organizational Security

Are responsibilities for asset protection and for carrying out specific information security processes clearly identified and communicated to the relevant parties?

YES

Are information security personnel (internal or outsourced) responsible for information security processes?

YES

Data center is following dedicated processes and procedure. Sage does have internal policies too.

Are information security personnel responsible for the creation, and review of information security policies?

YES

Sage does have internal security departments to create and review policies.

Are information security personnel responsible for the review and/or monitoring information security incidents or events?

YES

All events happened in the data center are reviewed. Automated monitoring is available for certain elements of the infrastructure.

Do all projects involving Scoped Systems and Data go through some form of information security assessment?

YES

Asset and Information Management

Is there an asset management program approved by management, communicated to constituents and an owner to maintain and review?

NO

No, however documents are held up to date to reflect the data center structure.

Is there an asset Inventory list or configuration management Database (CMDB)?

YES

Is there an acceptable use policy for information and associated assets that has been approved by management, communicated to appropriate Constituents and assigned an owner to maintain and periodically review the policy?

YES

Is there a process to verify return of constituent assets (computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination?

YES

All assets provided for and to Sage employees have to be returned once they are no longer needed. Either due to a change in work or termination of contract.

Is Information classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification?

YES

Is an owner assigned to all Information Assets?

NO

Are owners responsible to approve and periodically review access to Information Assets?

NO

Is there a policy or procedure for information handling (storing, processing, and communicating) consistent with its classification that has been approved by management, communicated to appropriate constituents and assigned an owner to maintain and periodically review?

YES

Does the policy or procedure for information handling include encryption requirements?

YES

Does the policy or procedure for information handling include storage requirements including authorized use of Public Cloud storage?

No public cloud storage.

NO

Does the policy or procedure for information handling include electronic transmission security requirements including email, web, and file transfer services?

emails are not encrypted. Communication to external systems is encrypted (e.g. https or sftp).

YES

Does the policy or procedure for information handling include removable media (Thumb Drives, DVDs, Tapes, etc.) requirements?

YES

Is there a data retention/destruction requirement that includes information on live media, backup/archived media, and information managed by Subcontractors?

In case hardware needs to be dismissed, an appropriate destruction mechanism is in place.

YES

Is Scoped Data sent or received via physical media?

NO

Is Scoped Data sent or received electronically?	YES
Is all Scoped Data sent or received electronically encrypted in transit while outside the network?	YES
Does Scoped Data sent or received electronically include protection against malicious code by network virus inspection or virus scan at the endpoint? Servers are employed with anti virus inspection.	YES
Do scans performed on incoming and outgoing email include phishing prevention?	YES
Are scoped systems or data stored or transferred in cloud-based public file sharing solutions? If yes, please explain in the 'Additional Information' field.	NO
Is regulated or confidential Scoped Data stored electronically?	YES
Is regulated or confidential Scoped Data stored in a database?	YES
Is regulated or confidential Scoped Data stored in files?	YES
Are encryption keys managed and maintained for Scoped Data?	YES
Are encryption keys generated in a manner consistent with key management industry standards?	YES

Is there an option for clients to manage their own encryption keys?

Exception: VPN

NO

Are Constituents able to view client's unencrypted Data?

Only admins/operations team has access due to maintainance.

YES

Do Constituents have the ability to view an unencrypted version of regulated or confidential Information?

Only admins/operations team has access due to maintainance.

YES

Human Resource Security

Are Human Resource policies approved by management, communicated to Constituents and an owner to maintain and review? Extract from police records are requested.	YES
Do Human Resource policies include Constituent background screening criteria?	YES
Does Constituent background screening criteria include Criminal screening?	YES
Are Constituents required to attend security awareness training?	YES
Does the security awareness training program include an explanation of Constituents' security roles and responsibilities?	YES
Does the security awareness training program include new hire and annual participation?	YES
Does the Human Resource policy include a disciplinary process for non-compliance?	YES
Does the Human Resource policy include Termination and/or change of status processes?	YES

Is electronic access to systems containing scoped data removed within 24 hours for terminated constituents?	YES
Is there a physical security program approved by management, communicated to constituents, and has an owner been assigned to maintain and review?	YES

Physical and Environmental Security

Are there physical security controls for all secured facilities (e.g., data centers, office buildings)?	YES
Do the physical security controls include electronic controlled access system (key card, token, fob, biometric reader, etc.)?	YES
Do the physical security controls include entry and exit doors alarmed (forced entry, propped open) and/or monitored by security guards?	YES
Are there physical access controls that include restricted access and logs kept of all access?	YES
Do physical access controls include collection of access equipment (badges, keys, change pin numbers, etc.) upon termination or status change?	YES
Are physical access control procedures documented?	YES
Do physical access controls require reporting of lost or stolen access cards/keys?	YES
Are there environmental controls (e.g., Fire detection and suppression) in secured facilities to protect computers and other physical assets?	YES

Are visitors permitted in the facility?	NO
Do the Scoped Systems and Data reside in a data center?	YES
Are locking screensavers on unattended system displays or locks on consoles required within the data center?	YES
Is there a procedure for equipment removal from the data center? Equipment is not allowed to be removed from the data center, unless it is destroyed.	YES

Operations Management

Are management approved operating procedures utilized?	YES
Is there an operational change management/Change Control policy or program that has been documented, approved by management, communicated to appropriate Constituents and assigned an owner to maintain and review the policy?	YES
Do changes to the production environment including network, systems, application updates, and code changes subject to the change control process?	YES
Does the change control process include a formal process to ensure clients are notified prior to changes being made which may impact their service? There are scheduled maintenance windows for upgrade/updating the systems and/or software. In case of additional maintenance windows, customers are informed.	YES
Does the change control process include a scheduled maintenance window?	YES
Does the change control process include a scheduled maintenance window which results in client downtime?	YES
Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?	YES

Are new, upgraded or enhanced systems required to include a determination of security requirements based on the sensitivity of the data?	YES
Do systems and network devices utilize a common time synchronization service?	YES

Access Control

Is there an access control program that has been approved by management, communicated to Constituents and an owner to maintain and review the program? Segregation of duty: Only a small number of employees have access to the data center.	YES
Are Constituents able to access Scoped Data? Only the operations team - not all employees of Sage.	NO
Are clients allowed to manage access to their own systems and data?	NO
Is there a set of rules governing the way IDs are created and assigned?	YES
Are unique IDs required for authentication to applications, operating systems, databases and network devices?	YES
Is there a process to request and receive approval for access to systems transmitting, processing or storing Scoped Systems and Data?	YES
Is access to applications, operating systems, databases, and network devices provisioned according to the principle of least privilege?	YES
Is there segregation of duties for granting access and approving access to Scoped Systems and Data?	YES

Is there segregation of duties for approving and implementing access requests for Scoped Systems and Data?	YES
Is access to systems that store or process scoped data limited?	YES
Are passwords used?	YES
Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms and network devices? If no, please explain in the 'Additional Information' field.	YES
Does the password policy apply to both Constituent and client passwords? If no, please explain in the 'Additional Information' field	YES
Does the password policy define specific length and complexity requirements for passwords?	YES
Does the password policy require a minimum password length of at least eight characters?	YES
Are complex passwords (mix of upper case letters, lower case letters, numbers, and special characters) required on systems transmitting, processing, or storing Scoped Data?	YES
Does the password policy prohibit a PIN or secret question as a possible stand-alone method of authentication?	NO

Does the password policy define requirements for provisioning and resetting passwords?	YES
Does the password policy require initial and temporary passwords to be changed upon next login?	YES
Does the password policy require initial and temporary passwords to be random and complex?	YES
Is password reset authority restricted to authorized persons and/or an automated password reset tool?	YES
Does the password policy require changing passwords at regular intervals?	YES
Does the password policy require keeping passwords confidential?	YES
Does the password policy prohibit users from sharing passwords?	YES
Does the password policy prohibit keeping an unencrypted record of passwords (paper, software file or handheld device)?	YES
Does the password policy prohibit including unencrypted passwords in automated logon processes (e.g., stored in a macro or function key)?	YES

Does the password policy require passwords to be encrypted in transit?	YES
Does the password policy require passwords to be encrypted or hashed in storage?	YES
Are user IDs and passwords communicated/distributed via separate media (e.g., e-mail and phone)?	YES
Does the password policy require changing passwords when there is an indication of possible system or password compromise?	YES
Is Multi-factor Authentication deployed?	YES
Does system policy require terminating or securing active sessions when finished?	YES
Does system policy require logoff from terminals, PC or servers when the session is finished?	YES
Is there a process for reviewing access?	YES
Are user access rights reviewed periodically?	YES
Are privileged user access rights reviewed periodically?	YES

Are access rights reviewed when a constituent changes roles?	YES
Are inactive Constituent user IDs disabled and deleted after defined periods of inactivity?	YES

Application Security

Are applications used to transmit, process or store Scoped Data?	YES
Are outside development resources utilized?	NO
Are system, vendor, or service accounts disallowed for normal operations and monitored for usage? Exception: operations team	YES
Are web applications configured to follow best practices or security guidelines (e.g., OWASP)?	YES
Is data input into applications validated?	YES
Are Scoped Systems and Data used in the test, development, or QA environments?	NO
Is application development performed?	YES
Is there a formal Software Development Life Cycle (SDLC) process?	YES
Is there a secure software development lifecycle policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	YES

Is there a documented change management/change control process for applications with Scoped Data?	YES
Does the application change management/change control process include change control procedures required for all changes to the production environment? In general, all changes follow through a change control procedures. However, a change in hard drive capacity is semi-automated and/or automated process. This change can and must also be performed on a live, up and running system. Such a change is not going through a change control procedure. All "real" changes, like "real" hardware setup/configuration as well as changes to the software go through a change control procedure.	NO
Does the application change management/change control process include testing prior to deployment?	YES
Does the application change management/change control process include stakeholder communication and/or approvals?	NO
Does the application change management/change control process include documentation for all system changes?	YES
Does the application change management/change control process include version control for all software?	YES
Does the application change management/change control process include logging of all Change Requests?	YES
Are applications evaluated from a security perspective prior to promotion to production?	YES

Is open source software or libraries used to transmit, process or store Scoped Data?	YES
Is a Secure Code Review performed regularly?	YES
Do secure code reviews include regular analysis of vulnerability to recent attacks?	YES
Are identified security vulnerabilities remediated prior to promotion to production?	YES
Does the SDLC process include communicating known un-remediated vulnerabilities to the Security Monitoring and Response group for awareness and monitoring? Such a group does not exist in general; vulnerabilities in the software are covered by the SDLC and vulnerabilities in the operations environment are tracked in the operations team.	N/A
Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?	YES
Do you have logical or Physical segregation between web, application and database components? i.e., Internet, DMZ, Database?	YES
Are Web Servers used for transmitting, processing or storing Scoped Data?	YES
Are reviews performed to validate compliance with documented web server software security standards?	NO

Is HTTPS enabled for all web pages?	YES
Are sample applications and scripts removed from web servers?	YES
Are available high-risk web server software security patches applied and verified at least monthly?	YES
Are web server software versions that no longer have security patches released prohibited?	YES
Is sufficient detail contained in Web Server and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?	YES
Are Web Server and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	YES
Is an API available to clients?	YES
Are mobile applications that access Scoped Systems and Data developed?	YES
Are any actions performed by the mobile application to access, process, transmit or locally store scoped systems and data?	YES

Is there an established incident management program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?	YES
Is there a formal Incident Response Plan?	YES
Does the Incident Response Plan include guidance for escalation procedure?	YES
Does the Incident Response Plan include actions to be taken in the event of an information security event?	YES
Are events on Scoped Systems or systems containing Scoped Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	YES
Are events on Scoped Systems or systems containing Scoped Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	YES
Does regular security monitoring include malware activity alerts such as uncleaned infections and suspicious activity?	YES
Is there an established business resiliency program that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the program? In case of critical events, the data center as procedures in place to provide continuous access to the application for the customer. Additionally the data center has a second, geographical independent, location to provide ongoing services. Annual "drills" are performed to guarantee such continuity.	YES

Does the business resiliency program include a formal annual (or more frequent) executive management review of business continuity key performance indicators, accomplishments, and issues?

YES

Do the products and/or services specified in the scope of this assessment fall within the scope of the Business Resiliency program?

In terms of Sage DPW: Remote working is possible to provide business continuity.

YES

Are formal business continuity procedures developed and documented?

In case of critical events, the data center as procedures in place to provide continuous access to the application for the customer. Additionally the data center has a second, geographical indepented, location to provide ongoing services. Annual "drills" are performed to guarantee such continuity.

YES

Has senior management assigned the responsibility for the overall management of critical response and recovery efforts?

YES

Is there a periodic (at least annual) review of your Business Resiliency procedures?

Data center: yes, due to ISAE3402

YES

Are there any dependencies on critical third party service providers?

The data center itself, which we use to provide our SaaS services.

YES

Is communication in the event of a disruption that impacts the delivery of key service provider products and services required?

YES

Is there a formal, documented Information Technology Disaster Recovery exercise and testing program in place?

YES

Is there an annual schedule of planned Disaster Recovery and other Business Resiliency exercises and tests? Tests are done once a year.	YES
Are backups of Scoped Systems and Data performed?	YES
Is there a policy or process for the backup of production data? 60 days of daily backups, backups are encrypted.	YES
Are backup media and restoration procedures tested at least annually?	YES
Are backup and replication errors reviewed and resolved as required?	YES
Is backup media stored offsite? There is a mirrored 2nd location for the main data center.	YES
Are backups containing Scoped Data stored in an environment where the security controls protecting them are equivalent to production environment security controls?	YES
Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements? We follow Austrian and EU law.	YES

Is there a documented process to identify and assess regulatory changes that could significantly affect the delivery of products and services?	YES
Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?	YES
Does the audit function have independence from the lines of business?	YES
Are audits performed to ensure compliance with applicable statutory, regulatory, contractual or industry requirements?	YES
Is there a set of policies and procedures that address required records management and compliance reporting?	YES
Are internal management reporting and/or external reporting to government agencies maintained in accordance with applicable law?	YES
Do employees undergo annual training regarding company expectations related to non-disclosure of insider information, code of conduct, conflicts of interest, and compliance and ethics responsibilities?	YES
Will this engagement include any call center related services? We have a Hotline, a client can call for help. However, we do not provide a call center service on behalf of our clients.	YES

Are marketing or selling activities conducted directly to Client's customers?	NO
Is training conducted for Constituents who have direct customer contact regarding consumer protection compliance responsibilities?	YES
Is there an incentive or compensation program for Constituents who directly sell/market to Client customers? If yes please describe in the 'Additional Information' field	NO
Are there documented policies and procedures to ensure compliance with applicable laws and regulations including Unfair, Deceptive, or Abusive Acts or Practices?	YES
Are collections activities conducted directly to Client's customers?	NO
Are terms of sale, dispute and/or return of goods procedures available online?	YES
Are there direct interactions with your client's customers?	NO
Is there a documented process to receive and respond to complaints, inquiries and requests from business or trade associations (e.g. BBB, GMOs, chambers of commerce, PCI Council) and from government agencies, including state attorneys general?	NO
Is there a documented escalation and resolution process to address specific complaints to management and the client?	YES

Are documented policies and procedures maintained to enforce applicable legal, regulatory or contractual cybersecurity obligations?	YES
Are client audits and/or risk assessments permitted?	YES
Is evidence of internal controls available during a client assessment?	YES
Are controls validated by independent, third party auditors or information security professionals?	YES
Is there a compliance program or set of policies and procedures that address internal and external Fraud Detection and Fraud Prevention?	YES
Are accounts opened, financial transactions initiated or other account maintenance activity (e.g., applying payments, address changes, receiving payments, transferring funds, etc.) through either electronic, telephonic, written or in-person requests made on behalf of your clients' customers?	NO
Are there policies and procedures to address payments compliance in the delivery of the product or services if required by regulation?	YES
Are electronic commerce web sites or applications used to transmit, process or store Scoped Systems and Data?	NO

Are all transaction details i.e., payment card info and information about the parties conducting transactions, prohibited from being stored in the Internet facing DMZ?	NO
Are policies and procedures in place to restrict activities or transactions for sanctioned countries (e.g. country blocking)?	YES
Are there compliance and sanction checks (e.g., Office of Foreign Assets Controls - OFAC) performed against customers, suppliers and third parties?	YES
Is there a sanctions compliance program or set of policies and procedures that address obligations for Office of Foreign Assets Controls (OFAC) requirements?	YES
Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data?	YES
Are end user device security configuration standards documented?	YES
Are Activity alerts such as uncleaned infections and suspicious activity reviewed and actioned at least weekly for all end user devices?	YES
Are defined procedures in place to identify and correct systems without anti-virus at least weekly for all end user devices?	YES

Are Constituents allowed to utilize mobile devices within your environment?	YES
Can Constituents access corporate e-mail using mobile devices?	YES
Is there a mobile device management program in place that has been approved by management and communicated to appropriate Constituents?	YES
Are personal computers (PCs) used to transmit, process or store Scoped Systems and Data.	YES
Are non-company managed PCs used to connect to the company network? Depends on the configuration and the demand of the client; in general, our SaaS-services are available on the internet. The SaaS-services can be e.g. connected via VPN to the company network to exchange files. So, in theory, a connection is established - however, not directly.	YES

Network Security

Is there a policy that defines network security requirements that is approved by management, communicated to Constituents and has an owner to maintain and review?	YES
Is there an approval process prior to installing a network device?	YES
Are there security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, Access control)?	YES
Are all network device administrative interfaces configured to require authentication and encryption?	YES
Are default passwords changed or disabled prior to placing network devices into production?	YES
Is there sufficient detail contained in network device logs to support incident investigation?	YES
Are all available high-risk security patches applied and verified on network devices?	YES
Are network technologies used to isolate critical and sensitive systems into network segments separate from those with less sensitive systems?	YES

Is every connection to an external network (e.g., The Internet, partner networks) terminated at a firewall?	YES
Do network devices deny all access by default?	YES
Do the firewalls have any rules that permit 'any' network, sub network, host, protocol or port on any of the firewalls (internal or external)? By default the web application can be accessed by everyone via https. However, this can be limited upon request of the customer.	YES
Is there a policy that defines the requirements for remote access from external networks to networks containing Scoped Systems and Data that has been approved by management and communicated to constituents?	YES
Are encrypted communications required for all remote network connections from external networks to networks containing Scoped Systems and Data?	YES
Is remote administration of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?	YES
Are encrypted communications required for all remote system access?	YES
Are Baseboard Management Controllers (BMCs) enabled on any servers or other devices?	YES

Is the default password changed on all BMCs?	YES
Are all BMCs configured on network address ranges reserved specifically for BMCs and no other devices?	YES
Are BMC firmware updates monitored regularly and applied at the first available maintenance window?	YES
Are Network Intrusion Detection capabilities employed? On Firewall level	YES
Is there a DMZ environment within the network that transmits, processes or stores Scoped Systems and Data?	YES
Are wireless networking devices connected to networks containing Scoped Systems and Data?	YES
Is there a wireless policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	YES
Does the Wireless Security Policy require wireless connections to be secured with WPA2, and encrypted using AES or CCMP?	YES

Privacy

Is there collection of, access to, processing of, or retention of any client scoped Data that includes any classification of non-public personal information or personal data of individuals?	YES
Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified as personally identifiable financial information under the Gramm-Leach-Bliley Act? We follow Austrian and EU law as well as the GDPR.	NO
Does the client scoped data include the disclosure of account numbers or identifiers to the consumer's account? For payroll payments the debit account information per employee is stored - in case the payroll module is used.	YES
Does the contract limit the usage of the account number information?	NO
Is client scoped data collected, accessed, processed, or retained that can be classified as consumer report information or derived from a consumer report under the Fair and Accurate Credit Reporting Act (FACTA)?	NO
Are policies and procedures for secure disposal of consumer information maintained to prevent the unauthorized access to or use of information in a consumer report or information derived from a consumer report?	YES

Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified as protected health information (PHI) or other higher healthcare classifications of privacy data under the U.S. Health Insurance Portability and Accountability Act?

N/A

No protected health information needed for the application itself; no explicit support for the U.S. Health Insurance Portability and Accountability Act.

Are there documented policies and procedures to detect and report unauthorized acquisition, use, or disclosure of PHI client scoped data?

N/A

No protected health information needed for the application itself; no explicit support for the U.S. Health Insurance Portability and Accountability Act.

Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified under U.S. State Privacy Regulations? (e.g., CA, MA, NY, NV, WA, CO)

N/A

No explicit support for U.S. State Privacy Regulations.

If client scoped data includes data of California residents, does the contract prohibit the vendor from retaining, using or disclosing the personal information for any other commercial purpose other than the specific purpose of performing the services?

N/A

No explicit support for U.S. State Privacy Regulations.

Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified as European Union covered Personal Data, or Sensitive Personal Data (e.g., genetic data, biometric data, health data)?

YES

Fully GDPR compliant

Is Client scoped data collected, transmitted, processed or retained that can be classified as Personal Information as defined by Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) or Canadian Provincial Privacy Regulations No explicit support for Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) or Canadian Provincial Privacy Regulations.	N/A
Are there contractual obligations and procedures defined to address breach notification to the client including maintenance of record-keeping obligations of all breaches? Fully GDPR compliant	YES
Is client scoped data collected, accessed, transmitted, processed or retained that can be classified as Cardholder Data (CHD) within a Cardholder Data Environment (CDE) for credit card processing?	NO
Is a Report on Compliance (ROC), or Self-Assessment Questionnaire (SAQ) and Attestation of Compliance for Service Providers (AOC) available? If Yes, Please provide and note in additional comments the type of third party assurance documentation	YES
Is client-scoped data of minors collected, transmitted, processed or stored that can be classified under the Children's Online Privacy Protection Act? for payroll purposes data of the children of employees are needed	YES
Does the organization maintain an external safe harbor certification for children's privacy? If yes, please indicate the certifying organization and link to current status	NO

Is there a designated organizational structure or function responsible for data privacy or data protection as it relates to client-scoped privacy data?	YES
Is documentation of data flows and/or data inventories maintained for client scoped privacy data based on data or asset classification? This is a task of the customer according to GDPR - however, we have templates.	NO
Is there a documented privacy policy and are procedures maintained for the protection of information collected, transmitted, processed, or maintained on behalf of the client?	NO
Are regular privacy impact risk assessments conducted? If yes, please provide frequency and scope in 'Additional Information' field. Once a year	YES
Is a Training and Awareness Program maintained that addresses data privacy and data protection obligations based on role? Once a year	YES
Does the organization have or maintain internet-facing websites(s), mobile applications, or other digital services or applications that, collect, use, or retain client-scoped private data and are used directly by individuals?	YES
Is personal data collected directly from an individual on behalf of the client?	YES

Are there documented privacy policies and procedures that address choice and consent based on the statutory, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data?	YES
For client-scoped Data, is personal data provided to the organization directly by the client?	YES
Are there documented policies and operating procedures regarding limiting the personal data collected and its use to the minimum necessary?	YES
Are there controls in place to ensure that the collection and usage of client scoped data or personal information used or processed by the organization is limited and in compliance with applicable law?	YES
Is there a documented records retention policy and process with defined schedules that ensure that Personal Information is retained for no longer than necessary?	YES
Are Individuals informed about their rights to access, review, update, and correct their personal information which is maintained by the organization?	YES
Are policies and procedures in place to address third party privacy obligations including limitations on disclosure and use of client scoped data?	YES
Do fourth-parties, (e.g., subcontractors, sub-processors, sub-service organizations) have access to or process client scoped data?	YES

Is there a documented data protection program with administrative, technical, and physical and environmental safeguards for the protection of client-scoped Data?	YES
Is there a documented policy or process to maintain accurate, complete and relevant records of client scoped data?	YES
Is there a data privacy or data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for client-scoped privacy data?	YES
Are there policies and processes in place to address privacy inquiries, complaints and disputes?	YES

Threat Management

Are Windows servers used as part of the Scoped Services?	YES
Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	YES
Does the anti-malware policy or program include defined operating systems that require antivirus?	YES
Does the approved anti-malware policy or program mandate an interval between the availability of a new anti-malware signature update and its deployment no longer than 24 hours?	NO
Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituent and an owner assigned to maintain and review the policy?	YES
Are network Vulnerability Scans performed against internal networks and systems?	YES
Are network vulnerability scans performed against internet-facing networks and systems?	YES
Do network Vulnerability Scans occur at least Monthly?	YES

Do you deliver software, firmware, and/or BIOS updates to clients through automatic downloads (e.g. Windows Update, LiveUpdate)?	YES
Is there a documented process in place to protect against and detect attacks against automatic software update mechanisms?	YES

Server Security

Are Servers used for transmitting, processing or storing Scoped Data?	YES
Are server security configuration standards documented and based on external industry or vendor guidance?	YES
Are server security configuration reviews performed regularly to validate compliance with documented standards?	YES
Are all servers configured according to security standards as part of the build process?	YES
Are all unnecessary/unused services uninstalled or disabled on all servers?	YES
Are vendor default passwords removed, disabled or changed prior to placing any device or system into production?	YES
Is sufficient detail contained in Operating System and application logs to support security incident investigations (at a minimum, successful and failed login attempts, and changes to sensitive configuration settings and files)?	YES
Are all systems and applications patched regularly?	YES

Are there any Operating System versions in use within the Scoped Services that no longer have patches released? If yes, please describe in the 'Additional Information' section.	NO
Is Unix or Linux used as part of the Scoped Services?	YES
Are users required to 'su' or 'sudo' into root?	YES
Are AS/400s used as part of the Scoped Services?	NO
Are Mainframes used as part of the Scoped Services?	NO
Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?	YES
Are Hypervisor hardening standards applied on all Hypervisors?	YES
Are Hypervisor Standard builds/security compliance checks required?	YES
Are Hypervisors kept up to date with current patches? Patchlevel -1 - for stability	YES
Are unnecessary/unused Hypervisor services turned off?	YES

Is sufficient information in Hypervisor logs to evaluate incidents?	YES
Are Containers (e.g., Docker, Kubernetes, OpenShift) used to process or store Scoped Data?	YES
Is there a Data Container Security policy approved by management, communicated to constituents and an owner to maintain and review?	YES

Cloud Hosting

Are Cloud Hosting services (IaaS) provided?	YES
Is there an Internet-accessible self-service portal available that allows clients to configure security settings and view access logs, security events and alerts?	NO
Are Cloud Hosting services subcontracted?	YES
Is there a management approved process to ensure that backup image snapshots containing Scoped Data are authorized by Outsourcer prior to being snapped? 60 day backup circle	YES
Are backup image snapshots containing Scoped Data stored in an environment where the security controls protecting them are commensurate with the production environment?	YES
Are default hardened base virtual images applied to virtualized operating systems?	NO
Does the Cloud Hosting Provider provide independent audit reports (e.g., Service Operational Control - SOC) for their cloud hosting services? ISAE3402 & ISO27001 is available	YES

Is the Cloud Service Provider certified by an independent third party for compliance with domestic or international control standards (e.g., the National Institute of Standards and Technology - NIST, the International Organization for Standardization - ISO)?

YES

ISAE3402 & ISO27001 is available

Die Sage GmbH ist mit der Sage DPW-Produktpalette führender Anbieter für Personalmanagement-Software in Österreich. Mit unserem umfassenden Produktportfolio bieten wir Softwarelösungen für alle Bereiche des Personalwesens. Sage DPW-Software ist bei rund 1.000 Kunden implementiert, vom mittelständischen bis zum multinationalen Unternehmen, in verschiedensten Branchen.

Sage GmbH
Stella-Klein-Löw-Weg 15
1020 Wien

+43 (0) 1 277 04
info@sagedpw.at