SITECORE

ANNEX A
TECHNICAL AND ORGANISATIONAL MEASURES

The technical and organizational security measures included in this Annex A apply to Sitecore's Managed Cloud, Sitecore EXM, Sitecore Content Hub, Sitecore XM Cloud, Sitecore Stream, Sitecore Experience Edge, Sitecore CDP, Sitecore Personalize, Sitecore Send, Sitecore Discover, Sitecore Search and Sitecore OrderCloud environments (collectively referred to as "**Processing Environments**"). These measures include controls designed to meet the high common level of cybersecurity mandated under **Directive (EU) 2022/2555 (NIS2)** for protecting network and information systems. Specifically, Sitecore's program addresses requirements for:

- Ensuring the availability, integrity, confidentiality, and resilience of processing systems and services.
- Implementing measures for risk analysis, incident detection and management, business continuity, and crisis response.
- Supporting timely and accurate notification to customers in the event of significant incidents affecting critical systems or services, as required under NIS2.

Further information on Sitecore's information security measures designed to protect information against loss of confidentiality, integrity, availability, and resilience can be found at:
https://www.sitecore.com/trust/security
https://www.sitecore.com/trust/privacy-policy

Sitecore maintains a robust security and data protection program that has been externally certified to meet rigorous international standards including ISO 27001, ISO 27017, ISO 27018, CSA STAR, and SOC 2. For more information, please visit https://www.sitecore.com/legal/compliance-certs.

The technical and organizational security measures applicable to Sitecore Connect (which embeds the Workato solution) can be found at: https://www.workato.com/legal/security.

The technical and organizational security measures applicable to Netlify can be found at: https://trust-centre.netlify-corp.com/

The term "**implemented**" refers to the existence of technical or procedural controls, designed to safeguard Customer Data and which are used to operate the Processing Environments.

Technical and Organizational Security Measure	Evidence
Measures of pseudonymisation and encryption of Customer Data	Sitecore has implemented the following measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking (e.g., database security, transmission security): (a) **Encryption:** Encryption mechanisms are used for data in storage+ and in transmission (e.g., TLS). Encryption is managed in accordance with industry best practices, including: (i) Maintaining secure encryption key management processes that require the encryption/decryption key to be: (A) Managed independently of the native operating system access control system; (B) Stored securely and adequately protected with strong access controls; (C) Secured during transmission or distribution; (D) Changed once keys have expired;

	(E) Retired or replaced if the integrity of the key has been or is reasonably believed to be weakened or compromised (which may include, depending on context, the departure of an individual with knowledge of the key); and (F) Whole disk encryption on all portable Sitecore systems containing Customer Data.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services	Sitecore has implemented and will maintain a comprehensive written information security program, designed to comply with applicable law, industry standards and best-practices. This program includes the following controls as part of its security governance: (a) **Objectives of the security program:** The security program will include appropriate administrative, logical, technical, physical, and organizational safeguards reasonably designed to: (i) Ensure the security, confidentiality, integrity, availability and resilience of Customer Data; (ii) To protect against any threats or hazards to the security or integrity of Customer Data in Sitecore's possession; and (iii) To prevent unauthorized or accidental access, destruction, loss, deletion, disclosure, alteration, or use of Customer Data. (b) **Certifications:** Sitecore maintains the current list of third party audited certifications on our website here: https://www.sitecore.com/legal/compliance-certs. (c) **Governance team:** Sitecore's Security Team, led by Sitecore's Data Protection and Security Council (composed of members of Sitecore's Executive Team), includes members of product security, legal, IT security, global workplace, security engineering and security operations. (d) **Processes:** Sitecore maintains several policies, including an Information Security Policy, designed to maintain consistent controls while governing Sitecore's security program. (e) **Risk assessment:** Sitecore maintains a risk assessment program to identify information security risks relating to its business, including IT systems, networks, product and business practices. (f) **Reviews:** This security program is reviewed at least annually or upon any material change in the provision of the Services to determine whether additional controls are to be implemented to address any new risks that such updates or business changes might introduce. (g) **Threat Intelligence:** Sitecore monitors threats and risks pertaining to the business to help identify threats that may require preventative action.
Measures for ensuring the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident	Sitecore has implemented the following measures to assure data security (physical/logical): (a) **Backup:** Secure backup procedures are maintained in its Processing Environments, including: (i) Storing backup media in an off-site, backup or alternate facility, with such facility being reviewed at least annually; (ii) Physically securing all backup media; and (iii) Maintaining inventory logs and inventories of backup media. (b) **Availability:** Processes are in place to monitor availability of systems in Sitecore's Processing Environments. (c) **Capacity Management:** Rules are in place to manage capacity in Sitecore's Processing Environments. (d) **Business Continuity and Disaster Recovery:** Sitecore has established Business Continuity Planning (BCP) and Disaster Recovery (DR) plans to ensure the service remains operational during disruptions. These plans include securely maintaining and testing alternate sites and infrastructure. Sitecore conducts annual BCP and DR tests to ensure our plans are current and effective.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Sitecore has established the following measures to implement and operate a secure network, i.e., operating system that has controls to protect the applications and data that it stores and processes: (a) **Malware and Intrusion Prevention:** This includes a hardened operating system with firewalls and anti-virus systems as appropriate to protect Sitecore's network, comprising the following controls: (i) Changing all manufacturer-supplied defaults before implementing into Processing Environments hosting, including but not limited to custom test accounts, default system

	or default user accounts, unnecessary functionality, and default encryption/decryption keys; (ii) Securing Sitecore systems according to industry accepted system hardening standards and keep current as change occurs in the Processing Environment; (iii) Running anti-malware and intrusion prevention controls on all systems operating in the Processing Environment; (iv) Anti-malware software is kept current and active, without the ability to be turned off or disabled. (v) Any system that is decommissioned (or repurposed for another Sitecore customer) must be sanitized in accordance with NIST 800-88, Guidelines for Media Sanitation; (vi) Servers in the Processing Environment must have technical controls to prohibit email usage and/or Internet browsing by end users; and (vii) All mobile devices (including laptops, tablets, or phones) used to access or store Customer Data must be secured with appropriate encryption. (b) **Vulnerability Management:** This includes a vulnerability management program, to detect and mitigate vulnerabilities in the platform in its Processing Environments comprising the following: (i) Sitecore uses a vulnerability scanning tool that complies with industry standards to validate security of Processing Environments; (ii) External scanning must occur at least quarterly; (iii) Internal scanning must occur at least monthly; (iv) Critical or High rated vulnerabilities will be addressed within 30 days of discovery; (v) Medium rated vulnerabilities will be addressed within 90 days of discovery; (vi) Low rated vulnerabilities will be addressed within 180 days of discovery; and (vii) Sitecore will promptly notify Customer if it becomes aware of the software containing a zero-day vulnerability that presents a high risk to Customer Data and shall provide details on any appropriate mitigation strategy. (c) **Security Monitoring:** A SIEM tool is used for 24x7 security monitoring.
Measures for user identification and authorisation	Sitecore has implemented the following technical (ID/password security) and organizational (user master data) measures for user identity management and authentication: (a) **Authentication and Authorization:** Controls are in place to secure authentication and authorize permission for access to Processing Environments, including utilizing: (i) A federated identity management solution is used for access to its Processing Environments, and where applicable, includes multifactor authentication mechanisms, including: (A) To secure delivery of data used to authenticate users during the user registration process. Emailed passwords must technically enforce one-time use. (B) Upon execution of a password reset, invalidate any previous sessions and redirect the user to the login page. (C) Unique IDs for access by Sitecore Employees to Processing Environments. Shared or "group" credentials for access to Processing Environments are prohibited. (D) Define and adhere to identity verification and appropriate workflow for access requests to Sitecore systems by its Personnel. (b) **Access controls:** Using centralized directory services, role-based access controls, which are reviewed quarterly, are used in Processing Environments to: (i) Immediately revoke access to Processing Environments of any Sitecore Personnel that is terminated or changes roles; (ii) Audit access lists to Processing Environments at least quarterly to ensure proper off boarding; (iii) Grant only the minimum access privileges required based upon the requestor's job responsibilities; (iv) Processing Environments must always deny user access by default and then build permission sets as needed; and

	(v) Logging requests for access to Sitecore systems and maintaining them in accordance with Sitecore's retention policies and must include relevant log information such as user ID, approving manager's name (where appropriate), timestamp, and description (where appropriate). (c) **Passwords:** Password security standards are used in its Processing Environments including: (i) Specified password complexity rules and length; (ii) Lockout policies for access attempts; (iii) Securely storing all account passwords used for oversight and management of Sitecore systems in an encrypted password vault; and (iv) Auditing user access to the aforementioned password vault and maintain relevant logs.
Measures for the protection of data during transmission	Sitecore has implemented procedures (Encryption Policy) to protect data during transmission to/from its Processing Environments. Data in motion is encrypted using Industry standard SSH/SCP or TLS 1.2 and above.
Measures for the protection of data during storage	Sitecore has implemented procedures (Encryption Policy) to protect data stored in its Processing Environments. All data captured is encrypted using 256-bit AES (Advanced Encryption Standard) encryption, one of the strongest block cyphers available.
Measures for ensuring physical security of locations at which Customer Data are processed	Sitecore has implemented the following technical and organizational measures to control access to our premises and facilities, particularly to check authorization: (a) **Access to premises and facilities:** Sitecore's Services are delivered in a Software-as-a-Service (SaaS) or Platform-as-a-Service (PaaS) model and hosted on third-party cloud infrastructure (e.g., Microsoft Azure, Amazon Web Services). While Sitecore does not directly manage the physical data center environments where Customer Data is stored or processed, Sitecore ensures that such environments are protected in accordance with the technical and organizational measures required under this DPA, via flow-down contractual commitments with its cloud infrastructure providers. This includes controls related to physical access, surveillance, and media destruction, which are implemented by the relevant hosting provider. Customers may review the certifications and physical security programs of our infrastructure partners at: • Microsoft Azure Compliance: https://learn.microsoft.com/en-us/azure/compliance/ • AWS Compliance Programs: https://aws.amazon.com/compliance/programs/ The following measures describe Sitecore's own physical access and security practices at its corporate offices and operational facilities, which do not host Customer Data. (b) **Physical security controls:** Physical security controls will be documented and maintained over all facilities where Customer Data is Processed to restrict access to servers, network ports, wireless access points, routers, firewalls, or any physical computing equipment involved in the provision of Services, including at a minimum, appropriate alarm systems, access controls, visitor access procedures, security guard force, fire suppression and CCTV video surveillance. (c) **Badge card access systems:** These are used to protect Processing Environments hosting Customer Data by limiting access to Sitecore premises to those with a badge card and valid entry of numerical code on control panels. (d) **Visitor Management:** Protocols designed to provide supervision of all visitors to Sitecore premises, both at reception areas and building entry points, are in place. This includes completion of NDA where appropriate, maintenance of visitor logs (with date, time duration, visitor name, company, and onsite personnel escort identification). (e) **CCTV:** Egress points and server rooms are subject to 24/7/365 video surveillance. (f) **Physical destruction:** Trash disposal programs that provide for the secure disposal of sensitive trash (any discarded material that contains or could disclose confidential information). Such secure disposal of data, including without limitation electronic media, will be performed in a manner that practicably prevents the information from being read or reconstructed such as: (i) For paper documents, destruction with a crosscut shredder; and

	(ii) For electronic media, degaussing and physical destruction in accordance with NIST Special Publication 800-88.
Measures for ensuring events logging	Sitecore has implemented procedures to maintain log activity in its Processing Environments, including: (a) Maintaining audit log events that identify a unique individual; (b) Maintaining audit logs showing all actions taken by any shared or generic user, such as administrator or root; (c) Protecting audit logs from unauthorized modification; (d) Audit logs must be promptly backed up to a central protected server; (e) Monitoring logs for security events, including but not limited to authentication logs, infrastructure audit logs, web application firewall logs; and (f) Taking steps so that all security events are promptly transmitted, investigated, and remediated by a security operations center.
Measures for ensuring system configuration, including default configuration	Sitecore has implemented formal change control processes while making changes to its Processing Environments are maintained. These processes are designed to: (a) Provide a consistent approach for controlling and identifying changes in the Processing Environment. (b) Define roles and responsibilities in a manner that allows for appropriate segregation of duties, to prevent fraud and potential malicious or accidental misuse of the Processing Environment.
Measures for internal IT and IT security governance and management	Sitecore maintains protocols to respond to any Security Incident in accordance with Customer requirements and pursuant to Data Protection Laws and Regulations: (a) **Security Incident Response Policy:** Sitecore maintains a Security Incident Response Policy. This details: (i) Incident response workflow, including stakeholders in the Security Incident Response Team ("**SIRT**"); (ii) Risk assessment/classification criteria; (iii) Notification procedures; and (iv) Protocols for engaging and co-operating with relevant law enforcement agencies or forensic analysts. (b) **SIRT:** Sitecore has a dedicated Security Incident Response Team to manage, respond and remediate to any security event or incident. (c) **SIRT Preparedness:** The SIRT will participate in regularly scheduled trainings to prepare for any Security Incident.
Measures for ensuring certification/assurance of processes and products.	See "Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services" above.
Measures for ensuring data minimisation	Sitecore has implemented the following measures to store data on data media (manual or electronic) and for subsequent checking (e.g., database security, transmission security): (a) **Data segregation:** Procedures are maintained to prevent unauthorized access of Customer Data by providing dedicated hosting resources for Customer Data in its managed Processing Environment. This ensures that Customer Data is always separate from data belonging to other customers. (b) **DLP:** Data loss prevention controls are used to prevent the unauthorized transmission (e.g., email transmission) and inadvertent loss of Customer information (e.g., USB encryption, mobile device management).
Measures for ensuring data quality	Sitecore has implemented the following measures to develop and implement secure software that has controls to protect the data that it stores and Processes: (a) **SDLC protocols:** Sitecore maintains a secure software development standard policy, which covers training, requirements, design, implementation, verification, release and response to prevent and mitigate vulnerabilities in software creation. Some of the measures in the SDLC protocols include:

	(i) Maintaining logical network segmentation between production and non-production environments. (ii) Strictly controlling access to application source code and associated items (designs, specifications, and validations plans) for Sitecore software to prevent the introduction of unauthorized functionality. (iii) Sitecore access credential passwords used for production and non-production environments will be different. (iv) Sitecore will not store Customer Data in non-production environments (development, testing, or staging environments). (v) Sitecore must review all application code for security and/or coding vulnerabilities prior to production deployment in Sitecore systems. Acceptable methods for code review include: (A) Static code testing tool (B) Dynamic code testing tool (C) Peer review (D) Tests must include coverage for: (E) Injection flaws (F) Buffer overflows (G) Insecure cryptographic storage (H) Improper error handling (I) Cross site scripting (J) Improper access controls (K) Cross-site request forgery (b) **Security implementation standards:** This includes which include security secure coding standards that address the OWASP Top 10 vulnerabilities within a testing environment prior to any external or Customer deployment. (c) **Penetration testing:** Sitecore conducts penetration testing (performed by a third-party) at least once per year and/or after any significant change in how the software is managed in the Processing Environment.
Measures for ensuring limited data retention	Sitecore has implemented procedures (Records Retention and Disposal Policy) to securely retain then delete Customer Data upon termination of the applicable contract and physical destruction when applicable.
Measures for ensuring accountability	Sitecore has implemented a data strategy to adapt to evolving security and Data Protection Laws and Regulations and has embedded robust data protection practices as part of our business culture. Strategic activities include: (a) Sitecore has established an internal Data Governance Team to encourage centralized discussion of Sitecore's strategic cross-functional privacy and security objectives, identify data governance risks and implement customer-oriented solutions. (b) The Data Governance Team is led by a Data Governance Committee (composed of Sitecore's Executive leadership team) to ensure top-down advisory and management oversight, policy approval and appropriate awareness of privacy and security across all sectors of our organization. (c) When possible, we have set a global baseline for data-handling practices, following the most protective Data Protection Laws and Regulations, to ensure equal rights to privacy. (d) Privacy is built into services as part of our Software Secure Development Lifecycle. (e) Implementing strong security protocols, conforming to the highest international security standards, with policies and operational processes overseeing all aspects of our business practices, allowing us to ensure data protection throughout the data lifecycle. (f) Understanding that employees are our first line of defense, Sitecore provides mandatory privacy, data protection and security training to all Sitecore employees, consultants and contractors. (g) We want to be transparent with our customers, partners, service providers and web visitors about how we handle data in all your interactions with Sitecore, and Process Personal Data only in accordance with specified instructions, as detailed in the Sitecore Privacy Policy.

	(h) Sitecore's Privacy Team continuously reviews and monitors applicable Data Protection Laws and Regulations, trends and developments so that changes required by applicable laws, or which are appropriate to our business are made proactively.
Measures for allowing data portability and ensuring erasure	Sitecore will support the right of return or deletion of data per section 8. Upon request, and apart from section 8, Customer may submit a request to receive a copy of their data.
Technical and organizational measures to be taken by the Data [sub]-processor to provide assistance to the Data Controller and, for transfers from a Data Processor to a Data [sub]-processor, to the Customer	Sitecore maintains a vendor management process for the selection, oversight and risk assessment of third-party suppliers, vendors (including Subprocessors): (a) **Due diligence:** All new suppliers and vendors (including Subprocessors) must be procured in accordance with Sitecore's Procurement Policy. This requires data review of privacy and security provisions by relevant stakeholders to assess and manage risk. (b) **Periodic assessments:** All existing suppliers and vendors (including Subprocessors) are subject to periodic assessment in accordance with Sitecore's procurement process. This requires data review of privacy and security provisions by relevant stakeholders to assess and manage risk.