GDPR Readiness report for AssistNow Inc

Generated on 11 February 2025

Report summary

This report provides a summary of AssistNow Inc's readiness posture for GDPR compliance as of 11th February 2025. Sprinto continuously monitors the security and readiness posture of AssistNow Inc to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. Below is a list of controls implemented by the organization to meet the compliance requirements. Sprinto achieves this by connecting to the systems, tools and policies of the company, and running continuous checks to determine the health of the controls.

Legend

- Check is healthy
- Check is work in progress

Chapter 1

General Provisions of GDPR

Article 1

GDPR Subject-matter and objectives

INTERNAL CONTROLS AND CHECKS

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy	✓

Article 3

Territorial scope

INTERNAL CONTROLS AND CHECKS

Control SDC 72

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Article 2

Material scope

INTERNAL CONTROLS AND CHECKS

Control SDC 72

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Article 4

Definitions of terms under GDPR

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Chapter 2

Principles related to processing of personal data

Article 8

Conditions applicable to child's consent in relation to information society services

INTERNAL CONTROLS AND CHECKS

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery ✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓
Vendor Management Procedure ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Article 5

Principles relating to processing of personal data

INTERNAL CONTROLS AND CHECKS

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Article 7

Conditions for consent

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Article 6

Lawfulness of processing

INTERNAL CONTROLS AND CHECKS

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically

Article 9

Processing of special categories of personal data

INTERNAL CONTROLS AND CHECKS

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Article 11

Processing which does not require identification

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles	⏱
Role based access should be setup	✓
Access Control Procedure	✓
HR Security Procedure	✓
HR Security Policy	✓
Access Control Policy	✓

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 5 checks

Offboarded staff access to critical systems should be revoked	✓

Access Control Procedure
HR Security Procedure
HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism
Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓
Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓
Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Article 10

Processing of personal data relating to criminal convictions and offences

INTERNAL CONTROLS AND CHECKS

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically	✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy	✓

Chapter 3

Rights of the Data Subject

Article 18

Right to restriction of processing

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure	✓
Access Control Policy	✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report	✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Article 16

Right to rectification

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

Article 23

Restrictions

INTERNAL CONTROLS AND CHECKS

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Article 22

Automated individual decision-making, including profiling

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

INTERNAL CONTROLS AND CHECKS

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 3 checks

Asset Management Policy	✓
Asset Management Procedure	✓
Encryption Policy	✓

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

Monitored via 1 check

Production systems should be secured with HTTPS	✓

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

Monitored via 2 checks

Operation Security Policy	✓
Operations Security Procedure	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓

Vendor Management Procedure

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 82**

Entity appoints a EU Representative to serve as a point of contact between EU authorities, data subjects and the organization

Monitored via 1 check

Appointment of an EU representative

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

Monitored via 1 check

Privacy By Design Policy 

Article 20

Right to data portability

INTERNAL CONTROLS AND CHECKS

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned 

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

INTERNAL CONTROLS AND CHECKS

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control SDC 114

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned 

Article 15

Right of access by the data subject

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map 

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Article 17

Right to erasure (‘right to be forgotten’)

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

Article 14

Information to be provided where personal data have not been obtained from the data subject

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map 

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner 

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned 

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

Article 13

Information to be provided where personal data are collected from the data subject

INTERNAL CONTROLS AND CHECKS

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

Article 21

Right to object

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Chapter 4

Controller and Processor

Article 29

Processing under the authority of the controller or processor

INTERNAL CONTROLS AND CHECKS

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Article 42

Certification

INTERNAL CONTROLS AND CHECKS

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Article 27

Representatives of controllers or processors not established in the Union

INTERNAL CONTROLS AND CHECKS

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control SDC 82

Entity appoints a EU Representative to serve as a point of contact between EU authorities, data subjects and the organization

Monitored via 1 check

Appointment of an EU representative

Control SDC 114

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Article 39

Tasks of the data protection officer

INTERNAL CONTROLS AND CHECKS

Control SDC 1

Entity has a documented policy to define behavioral standards and acceptable business conduct.

Monitored via 1 check

Code of Business Conduct Policy

Control SDC 6

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff 

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned 

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined 

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned 

Article 30

Records of processing activities

INTERNAL CONTROLS AND CHECKS

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control SDC 44

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running ✓
Endpoint Security Policy ✓
Asset Management Policy ✓
Physical and Environmental Security Procedure ✓
Asset Management Procedure ✓

Control SDC 49

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 3 checks

Asset Management Policy ✓
Asset Management Procedure ✓

Encryption Policy

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

Article 31

Cooperation with the supervisory authority

INTERNAL CONTROLS AND CHECKS

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management ✓

Control **SDC 82**

Entity appoints a EU Representative to serve as a point of contact between EU authorities, data subjects and the organization

Monitored via 1 check

Appointment of an EU representative ⏱

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity ✓

Incident Management Procedure ✓

Incident Management Policy ✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned ✓

Article 35

Data protection impact assessment

INTERNAL CONTROLS AND CHECKS

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically ✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically	✓
Risk Assessment & Management Policy	✓

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Article 37

Designation of the data protection officer

INTERNAL CONTROLS AND CHECKS

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned	✓

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit ✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned ✓

Article 26

Joint controllers

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy ✓

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control SDC 24

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management ✓

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control SDC 71

Entity has a documented policy outlining guidelines for the disposal and retention of information.

Monitored via 1 check

Data Retention Policy ✓

Article 34

Communication of a personal data breach to the data subject

INTERNAL CONTROLS AND CHECKS

Control SDC 53

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure ✓

Incident Management Policy ✓

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy ✓

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity ✓

Incident Management Procedure ✓

Incident Management Policy ✓

Article 38

Position of the data protection officer

INTERNAL CONTROLS AND CHECKS

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

Monitored via 1 check

Code of Business Conduct Policy ✓

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff ✓

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned ✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Article 40

Codes of conduct

INTERNAL CONTROLS AND CHECKS

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

Monitored via 1 check

Code of Business Conduct Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured	✓
HR Security Policy	✓

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff	✓
Staff should periodically acknowledge policies	✓

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 1 check

Information Security Policy	✓

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff	✓
HR Security Procedure	✓

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

Article 25

Data protection by design and by default

INTERNAL CONTROLS AND CHECKS

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

Monitored via 2 checks

Asset Management Policy

Asset Management Procedure

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

Monitored via 3 checks

Access to critical systems should be reviewed

Access Control Procedure

Access Control Policy

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity

Incident Management Procedure

Incident Management Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running	✓
Endpoint Security Policy	✓
Asset Management Policy	✓
Physical and Environmental Security Procedure	✓
Asset Management Procedure	✓

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 3 checks

Asset Management Policy	✓
Asset Management Procedure	✓
Encryption Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy	✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically	✓

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated	✓
Endpoint Security Policy	✓
Asset Management Policy	✓
Physical and Environmental Security Procedure	✓
Asset Management Procedure	✓

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly	⏱
Staff devices should have screen lock enabled	✓
Endpoint Security Policy	✓

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy	✓

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 3 checks

Asset Management Policy

Network Security Procedure

Asset Management Procedure

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

Operation Security Policy

SDLC Procedure

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 3 checks

Operation Security Policy

SDLC Procedure

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 3 checks

Operation Security Policy

SDLC Procedure

Operations Security Procedure

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

Monitored via 3 checks

Access Control Procedure

Acceptable Usage Policy

Access Control Policy

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

Control **SDC 1105**

Entity has documented guidelines on notifying customers and other stakeholders in case of a PII breach.

Monitored via 1 check

Personal Data Breach Notification Procedure ✓

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

Monitored via 1 check

Privacy By Design Policy ✓

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

Monitored via 3 checks

Data Breach Notification Policy ✓
Personal Data Breach Notification Procedure ✓
PHI Data breach Notification Procedure ✓

Article 33

Notification of a personal data breach to the supervisory authority

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 1 check

Information Security Policy 

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

Monitored via 1 check

Customer support page should be available 

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure 

Incident Management Policy 

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity 

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity	✓
Incident Management Procedure	✓
Incident Management Policy	✓

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan	✓
Business Continuity & Disaster Recovery Policy	✓

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan	✓
Business Continuity & Disaster Recovery Policy	✓

Article 43

Certification bodies

INTERNAL CONTROLS AND CHECKS

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned ✓

Article 24

Responsibility of the controller

INTERNAL CONTROLS AND CHECKS

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

Monitored via 2 checks

Asset Management Policy

Asset Management Procedure

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

Monitored via 3 checks

Access to critical systems should be reviewed

Access Control Procedure

Access Control Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity

Incident Management Procedure

Incident Management Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

Monitored via 2 checks

Operation Security Policy	✓
Operations Security Procedure	✓

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓
System Acquisition and Development Lifecycle Policy	✓

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

Monitored via 1 check

Data Classification Policy ✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned ✓

Article 28

Processor

INTERNAL CONTROLS AND CHECKS

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy ✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Article 32

Security of processing

INTERNAL CONTROLS AND CHECKS

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

Monitored via 2 checks

Asset Management Policy	✓
Asset Management Procedure	✓

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy	✓
Asset Management Policy	✓

Asset Management Procedure

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

Monitored via 3 checks

Access to critical systems should be reviewed

Access Control Procedure

Access Control Policy

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity

Incident Management Procedure

Incident Management Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan	✓
Business Continuity & Disaster Recovery Policy	✓

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically	✓
Risk Assessment & Management Policy	✓

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically	✓

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 3 checks

Asset Management Policy

Asset Management Procedure

Encryption Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

Monitored via 3 checks

Access Control Procedure

Acceptable Usage Policy

Access Control Policy

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

Monitored via 7 checks

Staff devices should have disk encryption enabled

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Acceptable Usage Policy

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 2 checks

Asset Management Policy

Asset Management Procedure

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly	
Staff devices should have screen lock enabled	✓
Endpoint Security Policy	✓

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy	✓

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 3 checks

Asset Management Policy	✓
Network Security Procedure	✓
Asset Management Procedure	✓

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

Monitored via 2 checks

Operation Security Policy	✓
Operations Security Procedure	✓

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

Monitored via 3 checks

Operation Security Policy	✓
Business Continuity Plan	✓
Operations Security Procedure	✓

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓
System Acquisition and Development Lifecycle Policy	✓

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit	✓

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management	✓

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned	✓

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 3 checks

Management Review of Internal Audit	✓
Senior management should be assigned	✓
Compliance Policy	✓

Control **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

Monitored via 3 checks

Organization chart should be reviewed by senior management	✓
HR Security Procedure	✓
HR Security Policy	✓

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management	✓
Risk Assessment & Management Policy	✓

Control **SDC 28**

Entity's Infosec officer reviews and approves the list of people with access to production console annually

Monitored via 1 check

Access to critical systems should be reviewed	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined	✓

Control **SDC 32**

Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.

Monitored via 4 checks

Org chart should be maintained ✓
Compliance Policy ✓
Compliance Procedure ✓
Information Security Policy ✓

Control **SDC 154**

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

Monitored via 1 check

Infrastructure operations person should be assigned ✓

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned ✓
HR Security Policy ✓

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

Monitored via 3 checks

Compliance program manager should be assigned	✓
Compliance Policy	✓
Compliance Procedure	✓

Control **SDC 395**

Entity has documented policies and procedures to facilitate the implementation of personnel security.

Monitored via 2 checks

HR Security Procedure	✓
HR Security Policy	✓

Control **SDC 119**

Entity has documented guidelines to manage communications protections and network security of critical systems.

Monitored via 2 checks

Network Security Procedure	✓
Communications & Network Security Policy	✓

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

Article 36

Prior consultation

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control SDC 68

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy

Vendor Management Procedure

Chapter 5

Transfers of personal data to third countries or international organisations

Article 46

Transfers subject to appropriate safeguards

INTERNAL CONTROLS AND CHECKS

Control SDC 388

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓

Vendor Management Procedure

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

Monitored via 1 check

Data Retention Policy

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

Monitored via 3 checks

Internal Audit
Asset Management Policy
Asset Management Procedure

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Procedure

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control SDC 381

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure	✓
Physical & Environmental Security Policy	✓

Article 44

General principle for transfers

INTERNAL CONTROLS AND CHECKS

Control SDC 74

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Article 45

Transfers on the basis of an adequacy decision

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Article 47

Binding corporate rules

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Article 49

Derogations for specific situations

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓

Vendor Management Policy

Article 50

International cooperation for the protection of personal data

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy ✓

Vendor Management Procedure ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Article 48

Transfers or disclosures not authorised by Union law

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management	✓
Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

About Sprinto

Sprinto is a modern platform for continuous compliance monitoring. It automates the detection, remediation, and management of security risks, ensuring ongoing compliance with leading security and privacy standards.