GDPR Readiness report for Product Fruits s.r.o.

Generated on 03 November 2023

Report summary

This report provides a summary of Product Fruits s.r.o.'s readiness posture for GDPR certification as of 3rd November 2023. Sprinto continuously monitors the security and readiness posture of Product Fruits s.r.o. to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. 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 **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined ✓

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 3

Territorial scope

INTERNAL CONTROLS AND CHECKS

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined 

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically 

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 2

Material scope

INTERNAL CONTROLS AND CHECKS

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 4

Definitions of terms under GDPR

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

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 **SPR 97**

Entity ensures that the Disaster Recovery Plan is tested periodically and learnings documented

Tested via 1 check

Disaster recovery ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 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

Tested via 1 check

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

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 79**

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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Article 5

Principles relating to processing of personal data

INTERNAL CONTROLS AND CHECKS

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner

Control **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report 

Article 7

Conditions for consent

INTERNAL CONTROLS AND CHECKS

Control **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map 

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner 

Control **SPR 79**

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

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 6

Lawfulness of processing

INTERNAL CONTROLS AND CHECKS

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically 

Control **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map 

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner 

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically 

Control SPR 79

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

Tested via 1 check

Risk assessment should be conducted periodically

Article 9

Processing of special categories of personal data

INTERNAL CONTROLS AND CHECKS

Control SPR 31

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

Tested via 1 check

Org policy should be defined

Control SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control SPR 77

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 79**

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

Tested via 1 check

Risk assessment should be conducted periodically

Article 11

Processing which does not require identification

INTERNAL CONTROLS AND CHECKS

Control **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined

Access control procedure should be defined

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓

Access to critical systems should be reviewed

Users of critical system should be identified

Control **SPR 44**

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

Tested via 1 check

Staff devices should have antivirus running

Article 10

Processing of personal data relating to criminal convictions and offences

INTERNAL CONTROLS AND CHECKS

Control **SPR 31**

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

Tested via 1 check

Org policy should be defined

Control **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 79**

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

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested 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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 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

Tested via 1 check

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

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 16

Right to rectification

INTERNAL CONTROLS AND CHECKS

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested via 1 check

Review of the privacy policy ✓

Article 23

Restrictions

INTERNAL CONTROLS AND CHECKS

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined ✓

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control SPR 114

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

Tested via 1 check

Privacy officer should be assigned

Control SPR 143

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 22

Automated individual decision-making, including profiling

INTERNAL CONTROLS AND CHECKS

Control SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control SPR 76

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

Tested via 1 check

Data consent using cookie banner 

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report 

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 12

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

INTERNAL CONTROLS AND CHECKS

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted

Control SPR 51

User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.

Tested via 1 check

Production systems should be secured with HTTPS

Control SPR 62

Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary

Tested via 1 check

Health of production infrastructure should be monitored

Control SPR 68

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

Tested via 1 check

Vendor management policy should be defined

Control SPR 77

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 82**

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

Tested via 1 check

Appointment of an EU representative

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested via 1 check

Review of the privacy policy

Control **SPR 433**

Entity has an established a policy which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations and makes it available to all staff members on the company employee portal

Tested via 1 check

Privacy by design policy should be defined 

Article 20

Right to data portability

INTERNAL CONTROLS AND CHECKS

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned 

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 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

Tested 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 **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 15

Right of access by the data subject

INTERNAL CONTROLS AND CHECKS

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 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

Tested via 1 check

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

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 17

Right to erasure (‘right to be forgotten’)

INTERNAL CONTROLS AND CHECKS

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested 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 **SPR 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

Tested via 1 check

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

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner ✓

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned ✓

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested 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 **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested via 1 check

Review of the privacy policy

Article 21

Right to object

INTERNAL CONTROLS AND CHECKS

Control **SPR 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

Tested via 1 check

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

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner ✓

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Chapter 4

Controller and Processor

Article 29

Processing under the authority of the controller or processor

INTERNAL CONTROLS AND CHECKS

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 42

Certification

INTERNAL CONTROLS AND CHECKS

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 27

Representatives of controllers or processors not established in the Union

INTERNAL CONTROLS AND CHECKS

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 82**

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

Tested via 1 check

Appointment of an EU representative

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned ✓

Article 39

Tasks of the data protection officer

INTERNAL CONTROLS AND CHECKS

Control **SPR 1**

Entity has established a policy to define behavioral standards and acceptable business conduct and makes it available to all staff members on the company employee portal

Tested via 1 check

Code of business conduct policy should be defined ✓

Control **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff ✓

Control **SPR 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.

Tested via 1 check

Information security officer should be assigned

Control **SPR 31**

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

Tested via 1 check

Org policy should be defined

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Article 30

Records of processing activities

INTERNAL CONTROLS AND CHECKS

Control **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SPR 44**

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

Tested via 1 check

Staff devices should have antivirus running

Control **SPR 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access

Tested via 1 check

Public access for infra assets should be restricted

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted

Control **SPR 52**

Entity maintains an inventory of infrastructure assets and segregates production assets from its staging/development assets

Tested via 1 check

Critical Infrastructure assets should be identified

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested via 1 check

Review of the privacy policy

Article 31

Cooperation with the supervisory authority

INTERNAL CONTROLS AND CHECKS

Control **SPR 13**

Entity makes all policies and procedures available to all staff members via the company employee portal

Tested via 0 checks

Control **SPR 24**

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

Tested via 1 check

Policies should be reviewed by senior management

Control **SPR 82**

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

Tested via 1 check

Appointment of an EU representative

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity

Control SPR 114

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

Tested via 1 check

Privacy officer should be assigned ✓

Article 35

Data protection impact assessment

INTERNAL CONTROLS AND CHECKS

Control SPR 72

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

Tested via 1 check

Data protection policy should be defined ✓

Control SPR 79

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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 37

Designation of the data protection officer

INTERNAL CONTROLS AND CHECKS

Control **SPR 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.

Tested via 1 check

Information security officer should be assigned

Control **SPR 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

Tested via 1 check

Internal Audit

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned

Article 26

Joint controllers

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 24**

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

Tested via 1 check

Policies should be reviewed by senior management

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 71**

Entity has a documented policy that establishes guidelines for Data Retention and makes it available for all staff on the company employee portal

Tested via 1 check

Data retention policy should be defined

Article 34

Communication of a personal data breach to the data subject

INTERNAL CONTROLS AND CHECKS

Control **SPR 52**

Entity maintains an inventory of infrastructure assets and segregates production assets from its staging/development assets

Tested via 1 check

Critical Infrastructure assets should be identified

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined

Incident management procedure should be defined

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity

Article 38

Position of the data protection officer

INTERNAL CONTROLS AND CHECKS

Control **SPR 1**

Entity has established a policy to define behavioral standards and acceptable business conduct and makes it available to all staff members on the company employee portal

Tested via 1 check

Code of business conduct policy should be defined

Control **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff

Control SPR 22

Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.

Tested via 1 check

Information security officer should be assigned

Control SPR 114

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

Tested via 1 check

Privacy officer should be assigned

Article 40

Codes of conduct

INTERNAL CONTROLS AND CHECKS

Control SPR 1

Entity has established a policy to define behavioral standards and acceptable business conduct and makes it available to all staff members on the company employee portal

Tested via 1 check

Code of business conduct policy should be defined

Control **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff

Control **SPR 31**

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

Tested via 1 check

Org policy should be defined

Control **SPR 7**

Entity has established an Information Security Awareness training, and its contents are available for all staff on the company employee portal.

Tested via 1 check

Security training provider should be configured

Control **SPR 12**

Entity requires that all staff members review and acknowledge company policies annually

Tested via 1 check

Staff should periodically acknowledge policies

Control **SPR 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

Tested via 1 check

Information security policy should be defined 

Control **SPR 387**

Entity requires that new staff members complete Information Security Awareness training upon hire

Tested via 1 check

Infosec training should be completed by new staff 

Control **SPR 388**

Entity requires that all staff members complete Information Security Awareness training annually

Tested via 1 check

Staff should periodically complete security training 

Article 25

Data protection by design and by default

INTERNAL CONTROLS AND CHECKS

Control **SPR 100**

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

Tested via 1 check

Critical Infrastructure assets should be identified

Control **SPR 104**

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined

Asset management procedure should be defined

Endpoint security policy should be defined

Control **SPR 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

Tested via 1 check

Access to critical systems should be reviewed

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity

Control **SPR 61**

Entity's infrastructure is configured to review and analyse audit events for anomalous or suspicious activity and threats

Tested via 1 check

Threat detection system should be enabled

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined

Business continuity & disaster recovery policy should be defined

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined

Business continuity & disaster recovery policy should be defined

Disaster recovery policy should be defined

Control **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access

Tested via 1 check

Public access for infra assets should be restricted

Control **SPR 44**

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

Tested via 1 check

Staff devices should have antivirus running

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

Control **SPR 79**

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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 46**

Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner

Tested via 1 check

Staff devices should have OS updated

Control **SPR 47**

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

Tested via 2 checks

Health of staff devices should be monitored

Staff devices should have screen lock enabled

Control **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined

Control **SPR 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.

Tested via 1 check

Infrastructure provider should be configured

Control **SPR 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

Tested via 2 checks

Vulnerability should be closed in SLA	✓
Vulnerability scanner should be enabled	✓

Control **SPR 56**

Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities

Tested via 1 check

Vulnerability should be closed in SLA	✓

Control **SPR 58**

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

Tested via 3 checks

Data backup policy should be defined	✓
Operation security policy should be defined	✓
Operations security procedure should be defined	✓

Control **SPR 64**

Entity has a documented policy and procedure to manage changes to its operating environment that includes critical information. Such documentation is available to all relevant Staff Members via the company employee portal

Tested via 4 checks

Change management policy should be defined ✓
Operations security procedure should be defined ✓
System acquisition and development lifecycle policy should be defined ✓
Sdlc procedure should be defined ✓

Control **SPR 65**

Entity uses a change management system to track, review and log all changes to the application code.

Tested via 2 checks

Change management repos should be classified ✓
Change management source should be configured ✓

Control **SPR 66**

Entity ensures that all planned changes undergo a review and approval process as per the guidelines documented in the policy and procedure defined to manage changes

Tested via 5 checks

Changes to production code should be reviewed by peers ✓
Peer review should be enabled in control systems ✓
Change requests should be reviewed by peers ✓
Operations security procedure should be defined ✓
Sdlc procedure should be defined ✓

Control **SPR 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

Tested via 4 checks

Acceptable usage policy should be defined	✓
Access control policy should be defined	✓
Access control procedure should be defined	✓
Password policy should be defined	✓

Control **SPR 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Control **SPR 24**

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

Tested via 1 check

Policies should be reviewed by senior management	✓

Article 33

Notification of a personal data breach to the supervisory authority

INTERNAL CONTROLS AND CHECKS

Control **SPR 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

Tested via 1 check

Information security policy should be defined 

Control **SPR 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.

Tested via 1 check

Customer support page should be available 

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined 

Incident management procedure should be defined 

Control **SPR 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

Tested via 1 check

Incidents should be investigated based on severity 

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

Article 43

Certification bodies

INTERNAL CONTROLS AND CHECKS

Control SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control SPR 114

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

Tested via 1 check

Privacy officer should be assigned

Article 24

Responsibility of the controller

INTERNAL CONTROLS AND CHECKS

Control SPR 100

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

Tested via 1 check

Critical Infrastructure assets should be identified

Control SPR 104

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined	✓
Asset management procedure should be defined	✓
Endpoint security policy should be defined	✓

Control **SPR 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

Tested via 1 check

Access to critical systems should be reviewed	✓

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically	✓

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity	✓

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

Control **SPR 61**

Entity's infrastructure is configured to review and analyse audit events for anomalous or suspicious activity and threats

Tested via 1 check

Threat detection system should be enabled	✓

Control **SPR 62**

Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary

Tested via 1 check

Health of production infrastructure should be monitored

Control **SPR 64**

Entity has a documented policy and procedure to manage changes to its operating environment that includes critical information. Such documentation is available to all relevant Staff Members via the company employee portal

Tested via 4 checks

Change management policy should be defined

Operations security procedure should be defined

System acquisition and development lifecycle policy should be defined

Sdlc procedure should be defined

Control **SPR 65**

Entity uses a change management system to track, review and log all changes to the application code.

Tested via 2 checks

Change management repos should be classified

Change management source should be configured

Control **SPR 70**

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

Tested via 1 check

Data classification policy should be defined

Control SPR 114

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

Tested via 1 check

Privacy officer should be assigned

Control SPR 143

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website

Tested via 0 checks

Article 28

Processor

INTERNAL CONTROLS AND CHECKS

Control SPR 77

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 98**

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

Tested via 1 check

Management review of contractual obligations

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 32

Security of processing

INTERNAL CONTROLS AND CHECKS

Control **SPR 100**

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

Tested via 1 check

Critical Infrastructure assets should be identified

Control **SPR 104**

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined

Asset management procedure should be defined

Endpoint security policy should be defined

Control **SPR 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

Tested via 1 check

Access to critical systems should be reviewed

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined

Business continuity & disaster recovery policy should be defined

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined

Business continuity & disaster recovery policy should be defined

Disaster recovery policy should be defined

Control **SPR 61**

Entity's infrastructure is configured to review and analyse audit events for anomalous or suspicious activity and threats

Tested via 1 check

Threat detection system should be enabled

Control **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 20**

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

Tested via 1 check

Risk assessment should be conducted periodically

Control **SPR 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access

Tested via 1 check

Public access for infra assets should be restricted

Control **SPR 44**

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

Tested via 1 check

Staff devices should have antivirus running

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

Control **SPR 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

Tested via 4 checks

Acceptable usage policy should be defined ✓
Access control policy should be defined ✓
Access control procedure should be defined ✓
Password policy should be defined ✓

Control **SPR 141**

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

Tested via 2 checks

Staff devices should have disk encryption enabled ✓
Health of staff devices should be monitored ✓

Control **SPR 11**

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

Tested via 1 check

Health of production infrastructure should be monitored 

Control **SPR 13**

Entity makes all policies and procedures available to all staff members via the company employee portal

Tested via 0 checks

Control **SPR 46**

Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner

Tested via 1 check

Staff devices should have OS updated 

Control **SPR 47**

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

Tested via 2 checks

Health of staff devices should be monitored 

Staff devices should have screen lock enabled 

Control **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined

Control **SPR 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.

Tested via 1 check

Infrastructure provider should be configured

Control **SPR 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

Tested via 2 checks

Vulnerability should be closed in SLA

Vulnerability scanner should be enabled

Control **SPR 56**

Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities

Tested via 1 check

Vulnerability should be closed in SLA

Control **SPR 58**

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

Tested via 3 checks

Data backup policy should be defined	✓
Operation security policy should be defined	✓
Operations security procedure should be defined	✓

Control **SPR 59**

Entity backs-up their production databases periodically

Tested via 1 check

Backup should be enabled on production database	✓

Control **SPR 60**

Entity's data backups are restored and tested annually

Tested via 1 check

Data backup restoration	✓

Control **SPR 64**

Entity has a documented policy and procedure to manage changes to its operating environment that includes critical information. Such documentation is available to all relevant Staff Members via the company employee portal

Tested via 4 checks

Change management policy should be defined	✓
Operations security procedure should be defined	✓

System acquisition and development lifecycle policy should be defined

Sdlc procedure should be defined

Control **SPR 65**

Entity uses a change management system to track, review and log all changes to the application code.

Tested via 2 checks

Change management repos should be classified

Change management source should be configured

Control **SPR 66**

Entity ensures that all planned changes undergo a review and approval process as per the guidelines documented in the policy and procedure defined to manage changes

Tested via 5 checks

Changes to production code should be reviewed by peers

Peer review should be enabled in control systems

Change requests should be reviewed by peers

Operations security procedure should be defined

Sdlc procedure should be defined

Control **SPR 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

Tested via 1 check

Internal Audit

Control SPR 24

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

Tested via 1 check

Policies should be reviewed by senior management

Control SPR 22

Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.

Tested via 1 check

Information security officer should be assigned

Control SPR 25

Entity's Senior Management reviews and approves the state of the Information Security program annually

Tested via 2 checks

Management Review of Internal Audit

Senior management should be assigned

Control SPR 26

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

Tested via 1 check

Organization chart should be reviewed by senior management

Control **SPR 27**

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

Tested via 1 check

Risk assessment should be reviewed by senior management

Control **SPR 28**

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

Tested via 1 check

Access to critical systems should be reviewed

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 31**

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

Tested via 1 check

Org policy should be defined

Control **SPR 32**

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

Tested via 2 checks

Isms information security roles & responsibilities should be defined ✓

Org chart should be maintained ✓

Control **SPR 154**

Entity appoints an owner of Infrastructure operations, who is responsible for all assets in the inventory

Tested via 1 check

Infrastructure operations person should be assigned ✓

Control **SPR 396**

Entity appoints a People Operations Officer to develop and drive forward all HR security-related strategies across the company

Tested via 1 check

People operations person should be assigned ✓

Control **SPR 397**

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

Tested via 1 check

Compliance program manager should be assigned ✓

Control **SPR 395**

Entity has a documented policy to manage personnel security and makes it available for all staff on the company employee portal

Tested via 2 checks

Hr security policy should be defined ✓

Hr security procedure should be defined ✓

Article 36

Prior consultation

INTERNAL CONTROLS AND CHECKS

Control **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined

Control SPR 68

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

Tested via 1 check

Vendor management policy should be defined

Chapter 5

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

INTERNAL CONTROLS AND CHECKS

Control SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 46

Transfers subject to appropriate safeguards

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control SPR 77

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control SPR 71

Entity has a documented policy that establishes guidelines for Data Retention and makes it available for all staff on the company employee portal

Tested via 1 check

Data retention policy should be defined

Control SPR 144

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested via 1 check

Review of the privacy policy

Control **SPR 383**

Entity requires that all staff members complete Information Security Awareness training annually.

Tested via 1 check

Staff should periodically complete security training

Control **SPR 389**

Entity maintains and periodically reviews the inventory of systems which are critical to security commitments and requirements

Tested via 3 checks

Internal Audit

Asset management policy should be defined

Asset management procedure should be defined

Control **SPR 390**

Entity maintains the inventory of endpoint assets and segregates assets with access to critical data from the others

Tested via 2 checks

Asset management procedure should be defined

Staff devices health should be monitored regularly

Control **SPR 391**

Entity has a documented policy to establish guidelines on managing technical vulnerabilities and makes it available for all staff on the company employee portal

Tested via 3 checks

Operation security policy should be defined	✓
Operations security procedure should be defined	✓
Vulnerability management policy should be defined	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

Control **SPR 394**

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

Tested via 1 check

Audit logs should exist	✓

Article 45

Transfers on the basis of an adequacy decision

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically 

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically 

Article 47

Binding corporate rules

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically 

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 49

Derogations for specific situations

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 50

International cooperation for the protection of personal data

INTERNAL CONTROLS AND CHECKS

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control SPR 77

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Article 48

Transfers or disclosures not authorised by Union law

INTERNAL CONTROLS AND CHECKS

Control SPR 21

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically

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.