AKITRA

Fastest Path to Customer Trust with Security Compliance Automation

CONFIDENTIAL REPORT

GDPR Self Attestation Audit Report

TRACKIER®

Trackier

July 12, 2025

Audit Date

July 12, 2024 to July 11, 2025
Next Audit Window: July 12,2025 to July 11,2026

Table of Contents

DISCLAIMER

Akitra, Inc.
830 Stewart Dr Ste 269, Sunnyvale, CA 94085

The purpose of the report is to verify the Trackier conformance with the implementation and effectiveness of security controls in accordance with GDPR. The content of this report applies only to matters, which were evident to Akitra auditor at the time of the audit within the audit scope. Akitra accepts no liability whatsoever for consequences to, or actions taken by, third parties as a result of or in reliance upon information contained in this report. This audit is based on a sampling process.

Self Attestation Audit Report

➢ Section 1: Organization Information

Company name:	**Trackier**
Contract Person:	Aman Khatri
Main address:	B1/H3 Ground Floor Mathura Road Mohan Cooperative Ind. Area Badarpur, New Delhi, Delhi - 110044
Address of other sites:	2035 Sunset Lake Road, Suite B-2, Newark New Castle County, Delaware 19702
Website:	https://trackier.com/
Total number of employees:	121
Total number of employees within the scope:	121

➢ Section 2: Audit information

Audit standard(s):	**GDPR**
Audit type:	**Self Attestation Audit**
Date(s) of audit(s):	July 12, 2025
Duration:	Point in time audit.
Audit team:	Akitra Internal Audit Team

Audit Summary

Total Controls	61
Exceptions	0
Last Policy Update	25 April, 2025
Next Review Due	27 December, 2025

➢ Section 3: System Description

INSTRUCTIONS:

DC 1: Company overview and types of products and services provided

Trackier uses advanced technology and a customer-first approach to help marketers across the globe build great products, create exceptional experiences, and preserve customer privacy. We have 3 different SaaS products
a) Apptrove - Mobile measurement platform - Tracks your app growth and creates a platform for you wherein you can integrate with different sets of partners and view results of the same.
b) Affnook - One powerful iGaming affiliate marketing platform to improve affiliate engagement, automate workflows, track performance, and deter fraud. All at one place.
c) Performance Marketing Platform - Track campaign metrics and manage payouts of different affiliates along with monitoring their performance

DC 2: The principal service commitments and system requirements

Our terms of service - https://Trackier.com/terms-of-service/

Privacy policy - https://Trackier.com/privacy-policy/

Our billing policy - https://Trackier.com/billing-policy/

Our SLAs

Working hours

- Indian Client - Mon - Fri - 11 am to 8 pm
- US & Europe Client - Mon - Fri - 11 am to 11 pm

Leave

- Inform the POCs 1 day before your leave
- Notify on the respective groups
- Update calendar meetings

Meeting Guidelines

- All the meetings should be booked on the Google calendar and should have a Fireflies recording attached to it (Post-ending of the call)
- After every call, a meeting summary should be posted on primary channels and an email should be drafted and sent within 3 working hours.
- In case you have been invited for a meeting, accept or decline the invite within 1 hour of that received invitation.
- In case you decline, mention the appropriate reason for it such as conflicting with another call etc.

Query from Client - End

- Acknowledge the query as soon as you encounter it
- Respond to the query
  a) Within 30 minutes if not in a meeting or call
  b) Within 60 mins if in a meeting or on a non-working day from 11 am to 7 pm
- Indian Client - If the client has a query at night or after 8 pm then the next reply or acknowledgement should be the next day before 11 am
- US or Europe Client - If the client has a query at night or after 11 pm then the next reply or acknowledgment should be the next day before 11 am
- Basic query resolution within 2 working hours
- In case of a bug - Share the status within 3 hours once resolved or unresolved

Feature Requests

Give an ETA for the feature building post consulting with the product team, and acknowledge the request message within 3 hours

DC 3: The components of the system used to provide the services

3.1 Primary Infrastructure and Applications:

Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Datastore	Data Type
Custom HR System	Employee records and	Purchased	SaaS with any OS	Zoho People	Employee information

	HR processes				
Finance System	Payroll data	Purchased	SaaS with any OS	Zoho Payroll	Employee’s payroll
Tech Team	Version Controlling	Purchased	SaaS with any OS	Github	Code hosting and sharing
Tech team	Build, test, and deploy their software.	Purchased	SaaS with any OS	Jenkins	Code Build
Billing Software	Customer’s billing	Developed	SaaS with any OS	CloudStuff Technology	To manage customer’s billing and invoice

3.2 People:

Trackier has a staff of 121 employees and contractors.

3.3 Security Processes and Procedures:

Privacy policy - https://Trackier.com/privacy-policy/

3.4 Data:

- Customer's personal data - Trackier do not track or store any customer's personal data without the consent from the client. The data is not passed along to any third-party tool and is stored as part of our databases with all necessary safety measures
- Login Password: The registration requires you to create a password for accessing Trackier services, which is confidential and sensitive information, collected and retained within the Trackier database. But the said sensitive information is just used by you as a Trackier user for gaining access to the services and is not used or accessed by Trackier or its affiliates/partners in any way.
- Financial Information: The Bank Details may be visible on the cheques couriered to us for payment of any services, but the complete bank account details are never noted down or processed for any reasons whatsoever, with us.

Though we recommend direct deposit of payments in our Bank Account either electronic transfer or by the drop of a cheque.

3.5 Third Party Access:

Trackier adheres to the General Data Protection Regulation (GDPR) by enforcing strict controls around third-party data access. Personally Identifiable Information (PII) is pseudonymized (e.g., hashing or truncating IP addresses) before storage or processing. Third-party vendors (e.g., Salesforce, Mixpanel, AWS) only process data based on explicit instructions under signed Data Processing Agreements (DPAs), ensuring compliance with Article 28 of GDPR. Access to production environments is limited to essential engineering personnel and requires documented approval. In case of vendor offboarding or service termination, Trackier ensures secure return or deletion of personal data. All third-party access is monitored and aligned with Trackier's data protection impact assessments (DPIAs).

3.6 System Boundaries: (Product lines/ LOBs/ brands)

Product list -

Trackier uses advanced technology and a customer-first approach to help marketers across the globe build great products, create exceptional experiences, and preserve customer privacy. We have 3 different SaaS products

a) **Apptrove** - Mobile measurement platform - Tracks your app growth and creates a platform for you wherein you can integrate with different sets of partners and view results of the same.

b) **Affnook** - One powerful iGaming affiliate marketing platform to improve affiliate engagement, automate workflows, track performance, and deter fraud. All at one place.

c) **Performance Marketing Platform** - Track campaign metrics and manage payouts of different affiliates along with monitoring their performance

DC 4: Disclosures about identified security incidents

Not received any such incident or notification for any major failure.

DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

Background Check Process (BC1)
Trackier conducts background verification for all internal employees as part of its hiring and onboarding process. These checks comply with relevant local and international laws and are tailored based on role criticality and information sensitivity. The process includes criminal history checks (where permitted), identity verification, and employment history validation using both automated tools and manual review.

Background Check Process (BC2)
For third-party vendors, consultants, or contractors with privileged or technical access to Trackier systems, background checks are a prerequisite. These parties must provide evidence of recent verification or undergo background checks facilitated by Trackier. The assessment is risk-based and focuses on verifying identity, criminal records, and past affiliations, ensuring all personnel accessing sensitive data meet Trackier's security standards.

DC 6: Complementary User Entity Controls (CUECs):

Trackier's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Trackier's services to be solely achieved by Trackier's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Trackier.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Trust IDs	Complementary User Entity Controls

CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by Organization systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to Organization's application keys and API keys for access to the web service API
CC6.3	Authorized users and their associated access are reviewed periodically
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to Organization.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to the Organization.

DC 7: Complementary Subservice Organization Controls (CSOCs):

Although the subservice organization has been **"carved out"** for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at GCP related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Trackier receives and reviews the GCP SOC 2 report annually. In addition, through its operational activities, Trackier management monitors the services performed by GCP to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of

changes planned at the hosting facility, and relay any issues or concerns to AWS/Google/Azure management.

It is not feasible for the criteria related to the System to be achieved solely by Trackier. Therefore, each user entity's internal control must be evaluated in conjunction with Trackier's controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	GCP is responsible for restricting data center access to authorized personnel.
CC6.4	GCP is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	GCP is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	GCP is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	GCP is responsible for overseeing the regular maintenance of environmental protections at data centers.

DC 8: Disclosures of significant changes in last 1 year

- None made

➢ Section 4: Audit Objective

This self-attestation serves to affirm that Trackier has implemented the necessary measures and practices to comply with GDPR. The objective is to provide transparency regarding our data protection efforts and to demonstrate our dedication to safeguarding personal data in accordance with regulatory requirements.

➢ Section 5: Scope

Our self-attestation covers the following key areas:

1. **Data Protection Policies:** Detailed descriptions of the data protection policies and procedures adopted by our organization.

2. **Data Processing Activities:** An overview of how we collect, process, and manage personal data, including the legal basis for processing and data retention practices.
3. **Data Subject Rights:** Procedures established to ensure that individuals can exercise their rights under the GDPR, including access, rectification, and erasure of personal data.

4. **Data Security Measures:** Description of the technical and organizational measures implemented to protect personal data against unauthorized access, alteration, or destruction.

5. **Training and Awareness:** Information on the training provided to staff to ensure awareness and understanding of GDPR requirements and data protection responsibilities.

➢ Section 6: Internal Auditor's Report

To: Trackier

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls based on our examination. The examination was conducted by Akitra.The following document provides a detailed account of your GDPR compliance efforts. We have approached this self-attestation with rigor and transparency.

An examination of the service organization's the suitability of the design and operating effectiveness of controls involves:

1. Obtaining an understanding of the service organization's service commitments and system requirements.

2. Assessing the risks that the controls were not suitably designed or did not operate effectively.

3. Performing procedures to obtain evidence about whether the controls are implanted as per standard criteria.

4. Testing the operating effectiveness of controls stated in the Audit Report to provide reasonable assurance that the service organization achieved its service commitments and system requirements

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

- Akitra Team

➢ Section 7: Audit Details

Article ID	Article	CTL ID	Control Description	Test Applied by the Service Auditor	Test Results
ART- 5	Principles relating to processing of personal data	CTL14	The organization performs a risk assessment to determine the data types that can be shared with a managed service provider.	Reviewed the Risk Assessment Policy, Vendor Management Policy, and Vendor Risk Assessment Report to verify risk assessments are performed to determine data types shareable with managed service providers.	No Exception
		CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL27	The organization defines external communication requirements for incidents, including: - information about external party dependencies - criteria for notification to external parties as required by the organization policy in the event of a security breach - contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) - provisions for updating and communicating	Reviewed the Breach Notification and Security Incident Response Policy to verify defined external communication requirements for incidents, including dependencies, notification criteria, authority contacts, and update provisions.	No Exception

			external communication requirement changes		
		CTL28	The organization defines the types of incidents that need to be managed, tracked and reported, including: - procedures for the identification and management of incidents - procedures for the resolution of confirmed incidents - key incident response systems - incident coordination and communication strategy - contact method for internal parties to report incidents - support team contact information - notification to relevant management in the event of a security breach - provisions for updating and communicating the plan - provisions for training of support team - preservation of incident information - management review and approval, (in accordance with frequency), or when major changes to the organization occur	Reviewed the Incident Tracker to verify definitions and procedures for incident management, tracking, reporting, communication, training, and management review.	No Exception
		CTL48	Changes to the production environment are implemented by authorized personnel.	Reviewed the Change Statement, Product Access List, and System Change Policy to verify that only authorized personnel implement changes to the production environment.	No Exception

		CTL53	The organization changes shared data encryption keys - at the end of the (organization-defined lifecycle period) - when keys are compromised - upon termination/transfer of employees with access to the keys	Encryption key management aligns with policy, addressing key lifecycle, compromise, and employee access termination	No Exception
		CTL62	The organization's data classification criteria are reviewed, approved by management, and communicated to authorized personnel (in accordance with the organization-defined frequency), the data security management determines the treatment of data according to its designated data classification level.	Reviewed the Data Classification Policy, Policy Review Notes, and Employee Training Status Report to verify management approval and communication of classification criteria; confirmed that training has been completed as required.	No Exception
		CTL63	Logical access provisioning to information systems requires approval from appropriate personnel.	Reviewed Access Control Policy and access proof to verify that logical access provisioning to information systems requires approval from authorized personnel.	No Exception
		CTL64	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	Reviewed access revoke records and asset return proof to verify that logical access is documented, communicated to management, and revoked promptly upon termination.	No Exception

		CTL67	Physical access that is no longer required in the event of a termination or role change is revoked. If applicable, temporary badges are returned prior to exiting the facility.	Access Removal Screenshot	No exception
		CTL125	The organization collects personal information that is limited and is consistent with its objectives	Reviewed the Data Privacy Policy to verify that personal information collected is limited and aligned with the organization's stated objectives.	No Exception
		CTL126	The organization has reviewed the personal information collected by different methods before they are implemented in order to confirm that personal information is obtained fairly	Reviewed the Data Privacy Policy to confirm procedures are in place to assess fairness of personal information collection methods prior to implementation.	No Exception
		CTL127	The organization has defined policies and procedures to confirm that third parties from whom personal information is collected are reliable sources that collect information fairly and lawfully	Reviewed the Data Privacy Policy to verify defined procedures for assessing third-party sources of personal information for fairness and lawful collection.	No Exception
		CTL128	The organization informs data subjects when additional information is acquired about them for its use	Reviewed the Data Privacy Policy to confirm that procedures exist for informing data subjects when additional personal information is obtained.	No Exception

		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Reviewed the Data Privacy and Retention Policies to verify that personal information is retained only as long as necessary to fulfill the stated purposes.	No Exception
		CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Reviewed the Data Privacy and Retention Policies to verify defined policies and procedures preventing erasure or destruction of personal information during the specified retention period.	No Exception
		CTL158	The organization collects complete, current and accurate personal information for the relevant purposes for which it is to be used, as defined in the agreements with data subjects	Reviewed the Data Privacy and Retention Policies to verify that procedures ensure collection of complete, current, and accurate personal information in line with agreements with data subjects.	No Exception

		CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Reviewed the Data Privacy and Retention Policies to verify the existence of a process for addressing privacy inquiries, complaints, and disputes.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of privacy complaints and disputes to the complainants.	No Exception
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives and control effectiveness.	No Exception
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment	No Exception

				with regulatory and internal privacy requirements.	
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception
ART- 6	Lawfulness of processing	CTL15	(In accordance with the organization-defined frequency), management reviews controls within third party assurance reports to ensure that they meet organizational requirements, if control gaps are identified in the assurance reports, management takes action to address impact the disclosed gaps have on the organization.	Reviewed the Vendor Management Policy and Vendor Risk Assessment Report to verify that management periodically reviews third-party assurance reports and takes action on identified control gaps.	No Exception
		CTL119	The entity has a defined procedure to inform the data subjects about their available choices with respect to the collection, use and disclosure of personal information	Reviewed Cookies Accept, Data Privacy Policy, Privacy Acknowledgement, and Terms Acknowledgement to verify procedures inform data subjects of their choices regarding collection, use, and disclosure of personal information.	No Exception

		CTL120	The entity has a procedure to inform the data subjects of the consequences of refusing to provide personal information for the purpose identified in the notice (this does not seem relevant to what the criterion requires -- it belongs with 3.2-1)	Reviewed the Privacy Acknowledgement and Data Privacy Policy to verify procedures inform data subjects of consequences of refusing to provide personal information for the purposes identified in the notice.	No Exception
		CTL121	The entity has obtained Implicit or explicit consent from data subjects at or before the time personal information is collected or soon thereafter	Reviewed the Data Privacy and Data Retention Policies to verify procedures for obtaining data subject consent and ensuring timely data deletion in line with regulatory requirements.	No Exception
		CTL122	The entity has obtained implicit or explicit consent prior to a new use or purpose, If personal information that was previously collected is to be used for purposes not previously mentioned in the privacy notice	Reviewed the Data Privacy and Retention Policies to confirm that procedures are in place for obtaining renewed consent before using previously collected personal data for new purposes not originally disclosed.	No Exception
		CTL123	The entity obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed	Reviewed the Data Privacy and Retention Policies to ensure that explicit consent mechanisms are defined for the	No Exception

				collection, use, or disclosure of sensitive personal information in compliance with regulatory requirements.	
		CTL124	The organization has the procedure to obtain consent before personal information is transferred to or from an individual's computer or similar device	Reviewed the Data Privacy and Retention Policies along with the Cookie Consent mechanism to verify that procedures exist for obtaining user consent prior to transferring personal information to or from an individual's device.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
ART- 7	Conditions for consent	CTL119	The entity has a defined procedure to inform the data subjects about their available choices with respect to the collection, use and disclosure of personal information	Reviewed Cookies Accept, Data Privacy Policy, Privacy Acknowledgement, and Terms Acknowledgement to verify procedures inform data subjects of their choices regarding collection, use, and disclosure of	No Exception

				personal information.	
		CTL120	The entity has a procedure to inform the data subjects of the consequences of refusing to provide personal information for the purpose identified in the notice (this does not seem relevant to what the criterion requires -- it belongs with 3.2-1)	Reviewed the Privacy Acknowledgement and Data Privacy Policy to verify procedures inform data subjects of consequences of refusing to provide personal information for the purposes identified in the notice.	No Exception
		CTL121	The entity has obtained Implicit or explicit consent from data subjects at or before the time personal information is collected or soon thereafter	Reviewed the Data Privacy and Data Retention Policies to verify procedures for obtaining data subject consent and ensuring timely data deletion in line with regulatory requirements.	No Exception
		CTL122	The entity has obtained implicit or explicit consent prior to a new use or purpose, If personal information that was previously collected is to be used for purposes not previously mentioned in the privacy notice	Reviewed the Data Privacy and Retention Policies to confirm that procedures are in place for obtaining renewed consent before using previously collected personal data for new purposes not originally disclosed.	No Exception

		CTL123	The entity obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed	Reviewed the Data Privacy and Retention Policies to ensure that explicit consent mechanisms are defined for the collection, use, or disclosure of sensitive personal information in compliance with regulatory requirements.	No Exception
		CTL124	The organization has the procedure to obtain consent before personal information is transferred to or from an individual's computer or similar device	Reviewed the Data Privacy and Retention Policies along with the Cookie Consent mechanism to verify that procedures exist for obtaining user consent prior to transferring personal information to or from an individual's device.	No Exception
		CTL129	The organization obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise	Reviewed the Data Privacy Policy to verify that procedures require obtaining explicit consent from data subjects before collecting, using, or disclosing sensitive personal information, unless legally exempt.	No Exception

		CTL130	The organization has defined objectives related to privacy for retaining documentation of explicit consent for the collection, use, or disclosure of sensitive personal information.	Reviewed the Data Privacy Policy to verify defined objectives for retaining documentation of explicit consent for sensitive personal information handling.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
ART- 8	Conditions applicable to child's consent in relation to information society services	CTL119	The entity has a defined procedure to inform the data subjects about their available choices with respect to the collection, use and disclosure of personal information	Reviewed Cookies Accept, Data Privacy Policy, Privacy Acknowledgement, and Terms Acknowledgement to verify procedures inform data subjects of their choices regarding collection, use, and disclosure of personal information.	No Exception
		CTL120	The entity has a procedure to inform the data subjects of the consequences of refusing to provide personal information for the purpose identified in the notice (this does not seem relevant to what the criterion requires -- it belongs with 3.2-1)	Reviewed the Privacy Acknowledgement and Data Privacy Policy to verify procedures inform data subjects of consequences of refusing to provide personal	No Exception

				information for the purposes identified in the notice.	
		CTL121	The entity has obtained Implicit or explicit consent from data subjects at or before the time personal information is collected or soon thereafter	Reviewed the Data Privacy and Data Retention Policies to verify procedures for obtaining data subject consent and ensuring timely data deletion in line with regulatory requirements.	No Exception
		CTL122	The entity has obtained implicit or explicit consent prior to a new use or purpose, If personal information that was previously collected is to be used for purposes not previously mentioned in the privacy notice	Reviewed the Data Privacy and Retention Policies to confirm that procedures are in place for obtaining renewed consent before using previously collected personal data for new purposes not originally disclosed.	No Exception
		CTL123	The entity obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed	Reviewed the Data Privacy and Retention Policies to ensure that explicit consent mechanisms are defined for the collection, use, or disclosure of sensitive personal information in compliance with regulatory requirements.	No Exception

		CTL124	The organization has the procedure to obtain consent before personal information is transferred to or from an individual's computer or similar device	Reviewed the Data Privacy and Retention Policies along with the Cookie Consent mechanism to verify that procedures exist for obtaining user consent prior to transferring personal information to or from an individual's device.	No Exception
ART- 9	Processing of special categories of personal data	CTL125	The organization collects personal information that is limited and is consistent with its objectives	Reviewed the Data Privacy Policy to verify that personal information collected is limited and aligned with the organization's stated objectives.	No Exception
		CTL126	The organization has reviewed the personal information collected by different methods before they are implemented in order to confirm that personal information is obtained fairly	Reviewed the Data Privacy Policy to confirm procedures are in place to assess fairness of personal information collection methods prior to implementation.	No Exception
		CTL127	The organization has defined policies and procedures to confirm that third parties from whom personal information is collected are reliable sources that collect information fairly and lawfully	Reviewed the Data Privacy Policy to verify defined procedures for assessing third-party sources of personal information for fairness and lawful collection.	No Exception

		CTL128	The organization informs data subjects when additional information is acquired about them for its use	Reviewed the Data Privacy Policy to confirm that procedures exist for informing data subjects when additional personal information is obtained.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
ART- 10	Processing of personal data relating to criminal convictions and offences	CTL125	The organization collects personal information that is limited and is consistent with its objectives	Reviewed the Data Privacy Policy to verify that personal information collected is limited and aligned with the organization's stated objectives.	No Exception
		CTL126	The organization has reviewed the personal information collected by different methods before they are implemented in order to confirm that personal information is obtained fairly	Reviewed the Data Privacy Policy to confirm procedures are in place to assess fairness of personal information collection methods prior to implementation.	No Exception
		CTL127	The organization has defined policies and procedures to confirm that third parties from whom personal information is collected are reliable sources that collect information fairly and lawfully	Reviewed the Data Privacy Policy to verify defined procedures for assessing third-party sources of personal information for	No Exception

				fairness and lawful collection.	
		CTL128	The organization informs data subjects when additional information is acquired about them for its use	Reviewed the Data Privacy Policy to confirm that procedures exist for informing data subjects when additional personal information is obtained.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
ART- 11	Processing which does not require identificatio n	CTL125	The organization collects personal information that is limited and is consistent with its objectives	Reviewed the Data Privacy Policy to verify that personal information collected is limited and aligned with the organization's stated objectives.	No Exception
		CTL126	The organization has reviewed the personal information collected by different methods before they are implemented in order to confirm that personal information is obtained fairly	Reviewed the Data Privacy Policy to confirm procedures are in place to assess fairness of personal information collection methods prior to implementation.	No Exception
		CTL127	The organization has defined policies and procedures to confirm that third parties from whom personal information is collected are reliable sources that collect information fairly	Reviewed the Data Privacy Policy to verify defined procedures for assessing third-party sources	No Exception

			and lawfully	of personal information for fairness and lawful collection.	
		CTL128	The organization informs data subjects when additional information is acquired about them for its use	Reviewed the Data Privacy Policy to confirm that procedures exist for informing data subjects when additional personal information is obtained.	No Exception
		CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Reviewed the Data Privacy and Retention Policies to verify that personal information is retained only as long as necessary to fulfill the stated purposes.	No Exception
		CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Reviewed the Data Privacy and Retention Policies to verify defined policies and procedures preventing erasure or destruction of personal information during the specified retention period.	No Exception
		CTL137	The organization maintains an authentication procedure to authenticate the identity of data subjects who request access to their personal information, prior to giving them access to that information	Reviewed the Data Privacy and Retention Policies to verify that authentication procedures are in place to confirm data subject identity before granting access to	No Exception

				personal information.	
		CTL138	The organization allows data subjects to determine whether it maintains personal information about them and, upon request, provides access to the information.	Reviewed the Data Privacy and Retention Policies to verify that data subjects can confirm if personal information is held and are provided access upon request.	No Exception
		CTL139	The organization provides personal information to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any	Reviewed the Data Privacy and Retention Policies to verify that personal information is provided to data subjects in an understandable format, within a reasonable timeframe, and at reasonable cost.	No Exception
		CTL140	The organization informs data subjects in a timely manner if they are denied access to their personal information when they request it, along with the reason for the denial, unless prohibited by law or regulation	Reviewed the Data Privacy and Retention Policies to verify procedures for timely notification to data subjects of access denial and reasons, unless prohibited by law or regulation.	No Exception
ART- 12	Transparent information, communication and modalities for the exercise of the rights of the data subject	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval	No Exception

				requirements are pre-defined based on associated risk.	
		CTL116	The organization provides a notice defining the purpose of collecting information from data subjects (users)	Data privacy policy	No Exception
		CTL117	The organization has a well-defined privacy notice which is conspicuous and uses clear language	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice is well-defined, conspicuous, and uses clear language.	No Exception
		CTL118	The organization's privacy notice describes the objectives of the entity and the activities covered by the notice	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice clearly describes the organization’s objectives and covered activities.	No Exception
		CTL137	The organization maintains an authentication procedure to authenticate the identity of data subjects who request access to their personal information, prior to giving them access to that information	Reviewed the Data Privacy and Retention Policies to verify that authentication procedures are in place to confirm data subject identity before granting access to personal information.	No Exception

		CTL138	The organization allows data subjects to determine whether it maintains personal information about them and, upon request, provides access to the information.	Reviewed the Data Privacy and Retention Policies to verify that data subjects can confirm if personal information is held and are provided access upon request.	No Exception
		CTL139	The organization provides personal information to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any	Reviewed the Data Privacy and Retention Policies to verify that personal information is provided to data subjects in an understandable format, within a reasonable timeframe, and at reasonable cost.	No Exception
		CTL140	The organization informs data subjects in a timely manner if they are denied access to their personal information when they request it, along with the reason for the denial, unless prohibited by law or regulation	Reviewed the Data Privacy and Retention Policies to verify procedures for timely notification to data subjects of access denial and reasons, unless prohibited by law or regulation.	No Exception
		CTL154	Remedial action is taken in response to the misuse of personal information	Reviewed the Breach Notification, Breach Policy, and Security Incident Response Policy to verify that remedial actions are defined and taken in response to the misuse of personal	No Exception

				information.	
		CTL155	The organization has defined a process for providing notice of breaches and incidents to the affected data subjects and, where appropriate or required, to regulators, to meet the objectives related to privacy.	Reviewed the Data Privacy Policy and Security Incident Response Policy to verify that processes are defined for notifying affected data subjects and regulators of breaches and incidents in alignment with privacy objectives.	No Exception
		CTL156	For each data subject, the organization tracks the personal information that it holds or that it has disclosed to a third party	Reviewed the Data Privacy and Retention Policies to verify that procedures exist for tracking personal information held or disclosed to third parties for each data subject.	No Exception
		CTL157	The organization has a defined procedure for responding to data subjects' requests for an accounting of personal information held and of disclosures of that information. Information related to the requests is identified and communicated to data subjects.	Reviewed the Data Privacy and Retention Policies to verify that procedures are defined for responding to data subjects' requests for information on personal data held and its disclosures.	No Exception
		CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Reviewed the Cookies Accept mechanism, Data Privacy Policy, and Privacy Acknowledgement to verify that privacy notices are	No Exception

				provided to data subjects at or before the time personal information is collected.	
ART- 13	Information to be provided where personal data are collected from the data subject	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL116	The organization provides a notice defining the purpose of collecting information from data subjects (users)	Data privacy policy	No Exception
		CTL117	The organization has a well-defined privacy notice which is conspicuous and uses clear language	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice is well-defined, conspicuous, and uses clear language.	No Exception
		CTL118	The organization's privacy notice describes the objectives of the entity and the activities covered by the notice	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice clearly describes the organization’s objectives and covered activities.	No Exception

		CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Reviewed the Cookies Accept mechanism, Data Privacy Policy, and Privacy Acknowledgement to verify that privacy notices are provided to data subjects at or before the time personal information is collected.	No Exception
ART- 14	Information to be provided where personal data have not been obtained from the data subject	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL116	The organization provides a notice defining the purpose of collecting information from data subjects (users)	Data privacy policy	No Exception
		CTL117	The organization has a well-defined privacy notice which is conspicuous and uses clear language	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice is well-defined, conspicuous, and uses clear language.	No Exception

		CTL118	The organization's privacy notice describes the objectives of the entity and the activities covered by the notice	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice clearly describes the organization’s objectives and covered activities.	No Exception
		CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Reviewed the Cookies Accept mechanism, Data Privacy Policy, and Privacy Acknowledgement to verify that privacy notices are provided to data subjects at or before the time personal information is collected.	No Exception
ART- 15	Right of access by the data subject	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL116	The organization provides a notice defining the purpose of collecting information from data subjects (users)	Data privacy policy	No Exception

		CTL117	The organization has a well-defined privacy notice which is conspicuous and uses clear language	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice is well-defined, conspicuous, and uses clear language.	No Exception
		CTL118	The organization's privacy notice describes the objectives of the entity and the activities covered by the notice	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice clearly describes the organization’s objectives and covered activities.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL137	The organization maintains an authentication procedure to authenticate the identity of data subjects who request access to their personal information, prior to giving them access to that information	Reviewed the Data Privacy and Retention Policies to verify that authentication procedures are in place to confirm data subject identity before granting access to personal information.	No Exception

		CTL138	The organization allows data subjects to determine whether it maintains personal information about them and, upon request, provides access to the information.	Reviewed the Data Privacy and Retention Policies to verify that data subjects can confirm if personal information is held and are provided access upon request.	No Exception
		CTL139	The organization provides personal information to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any	Reviewed the Data Privacy and Retention Policies to verify that personal information is provided to data subjects in an understandable format, within a reasonable timeframe, and at reasonable cost.	No Exception
		CTL140	The organization informs data subjects in a timely manner if they are denied access to their personal information when they request it, along with the reason for the denial, unless prohibited by law or regulation	Reviewed the Data Privacy and Retention Policies to verify procedures for timely notification to data subjects of access denial and reasons, unless prohibited by law or regulation.	No Exception
		CTL156	For each data subject, the organization tracks the personal information that it holds or that it has disclosed to a third party	Reviewed the Data Privacy and Retention Policies to verify that procedures exist for tracking personal information held or disclosed to third parties for each data subject.	No Exception

		CTL157	The organization has a defined procedure for responding to data subjects' requests for an accounting of personal information held and of disclosures of that information. Information related to the requests is identified and communicated to data subjects.	Reviewed the Data Privacy and Retention Policies to verify that procedures are defined for responding to data subjects' requests for information on personal data held and its disclosures.	No Exception
		CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Reviewed the Cookies Accept mechanism, Data Privacy Policy, and Privacy Acknowledgement to verify that privacy notices are provided to data subjects at or before the time personal information is collected.	No Exception
ART- 16	Right to rectification	CTL141	The organization has a legal, contractual right to deny data subjects' requests to access their personal information	Reviewed the Data Privacy and Retention Policies to verify that the organization has legal and contractual provisions to deny data subjects' access requests when applicable.	No Exception
		CTL143	Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal	Reviewed the Data Privacy and Retention Policies to verify that data subjects are informed in writing of denied correction requests, including reasons and appeal	No Exception

				procedures.	
		CTL216	When provided by data subjects, The organization updates or corrects personal information that it holds or has provided to third parties	Reviewed the Data Privacy and Retention Policies to verify procedures for updating or correcting personal information held or disclosed to third parties upon data subject request.	No Exception
ART- 17	Right to erasure ("right to be forgotten")	CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Reviewed the Data Privacy and Retention Policies to verify that personal information is retained only as long as necessary to fulfill the stated purposes.	No Exception
		CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Reviewed the Data Privacy and Retention Policies to verify defined policies and procedures preventing erasure or destruction of personal information during the specified retention period.	No Exception
		CTL135	The organization ensures that personal information which is longer retained by the organization is anonymized or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	Reviewed the Data Privacy and Retention Policies to verify that personal information retained beyond its retention period is anonymized or destroyed to prevent loss, theft,	No Exception

				misuse, or unauthorized access.	
		CTL136	The organization has defined policies and procedures to erase or otherwise destroy personal information that has been identified for destruction.	Reviewed the Data Retention Policy to verify defined policies and procedures for erasing or securely destroying personal information identified for destruction.	No Exception
		CTL215	The organization captures the request for deletion of personal information, and information related to the requests is identified and flagged for destruction to meet The organization's objectives related to privacy.	Reviewed the Data Privacy and Retention Policies to verify that requests for deletion of personal information are captured, identified, and flagged for destruction in accordance with privacy objectives.	No Exception
ART- 18	Right to restriction of processing	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL116	The organization provides a notice defining the purpose of collecting information from data subjects (users)	Data privacy policy	No Exception

		CTL117	The organization has a well-defined privacy notice which is conspicuous and uses clear language	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice is well-defined, conspicuous, and uses clear language.	No Exception
		CTL118	The organization's privacy notice describes the objectives of the entity and the activities covered by the notice	Reviewed the Data Privacy Policy and Employee Privacy Policy and Notice to verify the privacy notice clearly describes the organization’s objectives and covered activities.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Reviewed the Cookies Accept mechanism, Data Privacy Policy, and Privacy Acknowledgement to verify that privacy notices are provided to data subjects at or before the time personal information is collected.	No Exception

ART- 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL144	The organization has a procedure for communicating privacy policies or other specific instructions or requirements for handling personal information to third parties	Reviewed the Data Privacy and Retention Policies to verify procedures for communicating privacy policies and handling instructions to third parties.	No Exception
		CTL145	The organization has a procedure for providing personal information to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject	Reviewed the Data Privacy and Retention Policies to verify procedures ensuring personal information is provided to third parties solely for original purposes and only with implicit or explicit data subject consent.	No Exception
		CTL147	The organization has a procedure for disclosing personal information to third parties for new purposes or uses, but only with the prior explicit consent of data subjects	Reviewed the Data Privacy and Retention Policies to verify procedures requiring prior explicit consent from data subjects before disclosing personal	No Exception

				information to third parties for new purposes.	
		CTL148	The organization creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely	Reviewed the Data Privacy and Retention Policies to verify that procedures exist for maintaining complete, accurate, and timely records of authorized disclosures of personal information.	No Exception
		CTL156	For each data subject, the organization tracks the personal information that it holds or that it has disclosed to a third party	Reviewed the Data Privacy and Retention Policies to verify that procedures exist for tracking personal information held or disclosed to third parties for each data subject.	No Exception
		CTL157	The organization has a defined procedure for responding to data subjects' requests for an accounting of personal information held and of disclosures of that information. Information related to the requests is identified and communicated to data subjects.	Reviewed the Data Privacy and Retention Policies to verify that procedures are defined for responding to data subjects' requests for information on personal data held and its disclosures.	No Exception
		CTL217	Personal information is disclosed only to third parties who have agreements with The organization to protect personal information in a manner consistent with the relevant aspects of The	Reviewed the Data Privacy and Retention Policies to verify that personal information is disclosed only to	No Exception

			organization’s privacy notice	third parties with agreements ensuring protection consistent with the organization’s privacy notice.	
ART-20	Right to data portability	CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL137	The organization maintains an authentication procedure to authenticate the identity of data subjects who request access to their personal information, prior to giving them access to that information	Reviewed the Data Privacy and Retention Policies to verify that authentication procedures are in place to confirm data subject identity before granting access to personal information.	No Exception
		CTL138	The organization allows data subjects to determine whether it maintains personal information about them and, upon request, provides access to the information.	Reviewed the Data Privacy and Retention Policies to verify that data subjects can confirm if personal information is held and are provided access upon request.	No Exception
		CTL139	The organization provides personal information to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any	Reviewed the Data Privacy and Retention Policies to verify that personal information is provided to data	No Exception

				subjects in an understandable format, within a reasonable timeframe, and at reasonable cost.	
		CTL140	The organization informs data subjects in a timely manner if they are denied access to their personal information when they request it, along with the reason for the denial, unless prohibited by law or regulation	Reviewed the Data Privacy and Retention Policies to verify procedures for timely notification to data subjects of access denial and reasons, unless prohibited by law or regulation.	No Exception
ART-21	Right to object	CTL119	The entity has a defined procedure to inform the data subjects about their available choices with respect to the collection, use and disclosure of personal information	Reviewed Cookies Accept, Data Privacy Policy, Privacy Acknowledgement, and Terms Acknowledgement to verify procedures inform data subjects of their choices regarding collection, use, and disclosure of personal information.	No Exception
		CTL120	The entity has a procedure to inform the data subjects of the consequences of refusing to provide personal information for the purpose identified in the notice (this does not seem relevant to what the criterion requires -- it belongs with 3.2-1)	Reviewed the Privacy Acknowledgement and Data Privacy Policy to verify procedures inform data subjects of consequences of refusing to provide personal information for the purposes identified in the notice.	No Exception

		CTL121	The entity has obtained Implicit or explicit consent from data subjects at or before the time personal information is collected or soon thereafter	Reviewed the Data Privacy and Data Retention Policies to verify procedures for obtaining data subject consent and ensuring timely data deletion in line with regulatory requirements.	No Exception
		CTL122	The entity has obtained implicit or explicit consent prior to a new use or purpose, If personal information that was previously collected is to be used for purposes not previously mentioned in the privacy notice	Reviewed the Data Privacy and Retention Policies to confirm that procedures are in place for obtaining renewed consent before using previously collected personal data for new purposes not originally disclosed.	No Exception
		CTL123	The entity obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed	Reviewed the Data Privacy and Retention Policies to ensure that explicit consent mechanisms are defined for the collection, use, or disclosure of sensitive personal information in compliance with regulatory requirements.	No Exception
		CTL124	The organization has the procedure to obtain consent before personal information is transferred to or from an individual's computer or similar device	Reviewed the Data Privacy and Retention Policies along with the Cookie Consent mechanism to	No Exception

				verify that procedures exist for obtaining user consent prior to transferring personal information to or from an individual's device.	
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Reviewed the Cookies Accept mechanism, Data Privacy Policy, and Privacy Acknowledgement to verify that privacy notices are provided to data subjects at or before the time personal information is collected.	No Exception
ART-22	Automated individual decision-making, including profiling	CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception

		CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Reviewed the Data Privacy and Retention Policies to verify the existence of a process for addressing privacy inquiries, complaints, and disputes.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of privacy complaints and disputes to the complainants.	No Exception
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives and control effectiveness.	No Exception
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment	No Exception

				with regulatory and internal privacy requirements.	
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception
ART-24	Responsibility of the controller	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
		CTL11	(The organization-defined security leader) conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Reviewed Security Review Meeting Minutes to verify that the designated security leader conducts periodic staff meetings to communicate security threats, program performance, and resource priorities.	No Exception
		CTL20	The design and operating effectiveness of internal controls are continuously evaluated against the established (organization-defined controls framework) by the	Reviewed the Risk Assessment Policy and Risk Assessment Report to verify continuous evaluation of	No Exception

			organization. Corrective actions related to identified deficiencies are tracked to resolution.	internal controls against the controls framework and tracking of corrective actions to resolution.	
		CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Reviewed the Data Privacy and Retention Policies to verify the existence of a process for addressing privacy inquiries, complaints, and disputes.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of privacy complaints and disputes to the complainants.	No Exception
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives and control effectiveness.	No Exception
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has	No Exception

				documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment with regulatory and internal privacy requirements.	
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception
ART-25	Data protection by design and by default	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
		CTL11	(The organization-defined security leader) conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Reviewed Security Review Meeting Minutes to verify that the designated security leader conducts periodic staff meetings to communicate security threats, program performance, and resource priorities.	No Exception

		CTL20	The design and operating effectiveness of internal controls are continuously evaluated against the established (organization-defined controls framework) by the organization. Corrective actions related to identified deficiencies are tracked to resolution.	Reviewed the Risk Assessment Policy and Risk Assessment Report to verify continuous evaluation of internal controls against the controls framework and tracking of corrective actions to resolution.	No Exception
		CTL125	The organization collects personal information that is limited and is consistent with its objectives	Reviewed the Data Privacy Policy to verify that personal information collected is limited and aligned with the organization's stated objectives.	No Exception
		CTL126	The organization has reviewed the personal information collected by different methods before they are implemented in order to confirm that personal information is obtained fairly	Reviewed the Data Privacy Policy to confirm procedures are in place to assess fairness of personal information collection methods prior to implementation.	No Exception
		CTL127	The organization has defined policies and procedures to confirm that third parties from whom personal information is collected are reliable sources that collect information fairly and lawfully	Reviewed the Data Privacy Policy to verify defined procedures for assessing third-party sources of personal information for fairness and lawful collection.	No Exception

		CTL128	The organization informs data subjects when additional information is acquired about them for its use	Reviewed the Data Privacy Policy to confirm that procedures exist for informing data subjects when additional personal information is obtained.	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Reviewed the Data Privacy and Retention Policies to verify that personal information is retained only as long as necessary to fulfill the stated purposes.	No Exception
		CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Reviewed the Data Privacy and Retention Policies to verify defined policies and procedures preventing erasure or destruction of personal information during the specified retention period.	No Exception

		CTL135	The organization ensures that personal information which is longer retained by the organization is anonymized or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	Reviewed the Data Privacy and Retention Policies to verify that personal information retained beyond its retention period is anonymized or destroyed to prevent loss, theft, misuse, or unauthorized access.	No Exception
		CTL136	The organization has defined policies and procedures to erase or otherwise destroy personal information that has been identified for destruction.	Reviewed the Data Retention Policy to verify defined policies and procedures for erasing or securely destroying personal information identified for destruction.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of privacy complaints and disputes to the complainants.	No Exception
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives	No Exception

				and control effectiveness.	
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment with regulatory and internal privacy requirements.	No Exception
		CTL215	The organization captures the request for deletion of personal information, and information related to the requests is identified and flagged for destruction to meet The organization's objectives related to privacy.	Reviewed the Data Privacy and Retention Policies to verify that requests for deletion of personal information are captured, identified, and flagged for destruction in accordance with privacy objectives.	No Exception
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception

ART-26	Joint Controller	CTL150	The organization has an agreement in place with third parties for disclosure of personal information to those parties.	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify that agreements with third parties include provisions for the disclosure of personal information.	No Exception
		CTL151	The organization has defined a process for assessment of vendors' and other third parties' compliance with personal information disclosure terms, and has defined remedial action in response to the misuse of that personal information	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify defined processes for assessing third-party compliance with personal information disclosure terms and specified remedial actions for misuse.	No Exception
ART-27	Representatives of controllers or processors not established in the Union	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
ART-28	Processor	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles,	No Exception

			risk associated with change scope and type.	workflows, notifications, and approval requirements are pre-defined based on associated risk.	
		CTL150	The organization has an agreement in place with third parties for disclosure of personal information to those parties.	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify that agreements with third parties include provisions for the disclosure of personal information.	No Exception
		CTL151	The organization has defined a process for assessment of vendors' and other third parties' compliance with personal information disclosure terms, and has defined remedial action in response to the misuse of that personal information	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify defined processes for assessing third-party compliance with personal information disclosure terms and specified remedial actions for misuse.	No Exception
ART-29	Processing under the authority of the controller or processor	CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception

ART-31	Cooperation with the supervisory authority	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
ART-32	Security of processing	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
		CTL11	(The organization-defined security leader) conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Reviewed Security Review Meeting Minutes to verify that the designated security leader conducts periodic staff meetings to communicate security threats, program performance, and resource priorities.	No Exception
		CTL20	The design and operating effectiveness of internal controls are continuously evaluated against the established (organization-defined controls framework) by the organization. Corrective actions related to identified deficiencies are tracked to	Reviewed the Risk Assessment Policy and Risk Assessment Report to verify continuous evaluation of internal controls against the controls framework	No Exception

			resolution.	and tracking of corrective actions to resolution.	
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Reviewed the Data Privacy and Retention Policies to verify the existence of a process for addressing privacy inquiries, complaints, and disputes.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of privacy complaints and disputes to the complainants.	No Exception
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives	No Exception

				and control effectiveness.	
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment with regulatory and internal privacy requirements.	No Exception
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception
ART-33	Notification of a personal data breach to the supervisory authority	CTL149	The organization creates and maintains a record of detected or reported unauthorized disclosures of personal information	Reviewed the Data Privacy and Retention Policies to verify procedures for recording detected or reported unauthorized disclosures of personal information.	No Exception
		CTL152	Organization takes remedial action in response to unauthorized disclosure of personal information by vendors and other third parties	Reviewed the Data Privacy and Retention Policies to verify that remedial actions are defined for	No Exception

				unauthorized disclosures of personal information by vendors and third parties.	
		CTL153	Organization maintains agreements with its vendors and other third parties, which require notifying the organization in the event of any actual or suspected misuse of personal information	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify that third-party agreements require notification of any actual or suspected misuse of personal information.	No Exception
		CTL154	Remedial action is taken in response to the misuse of personal information	Reviewed the Breach Notification, Breach Policy, and Security Incident Response Policy to verify that remedial actions are defined and taken in response to the misuse of personal information.	No Exception
		CTL155	The organization has defined a process for providing notice of breaches and incidents to the affected data subjects and, where appropriate or required, to regulators, to meet the objectives related to privacy.	Reviewed the Data Privacy Policy and Security Incident Response Policy to verify that processes are defined for notifying affected data subjects and regulators of breaches and incidents in alignment with privacy objectives.	No Exception

ART-34	Communication of a personal data breach to the data subject	CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
		CTL27	The organization defines external communication requirements for incidents, including: - information about external party dependencies - criteria for notification to external parties as required by the organization policy in the event of a security breach - contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) - provisions for updating and communicating external communication requirement changes	Reviewed the Breach Notification and Security Incident Response Policy to verify defined external communication requirements for incidents, including dependencies, notification criteria, authority contacts, and update provisions.	No Exception
		CTL154	Remedial action is taken in response to the misuse of personal information	Reviewed the Breach Notification, Breach Policy, and Security Incident Response Policy to verify that remedial actions are defined and taken in response to the misuse of personal information.	No Exception

		CTL155	The organization has defined a process for providing notice of breaches and incidents to the affected data subjects and, where appropriate or required, to regulators, to meet the objectives related to privacy.	Reviewed the Data Privacy Policy and Security Incident Response Policy to verify that processes are defined for notifying affected data subjects and regulators of breaches and incidents in alignment with privacy objectives.	No Exception
ART-35	Data protection impact assessment	CTL14	The organization performs a risk assessment to determine the data types that can be shared with a managed service provider.	Reviewed the Risk Assessment Policy, Vendor Management Policy, and Vendor Risk Assessment Report to verify risk assessments are performed to determine data types shareable with managed service providers.	No Exception
		CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Reviewed the Data Privacy and Retention Policies to verify the existence of a process for addressing privacy inquiries, complaints, and disputes.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of	No Exception

				privacy complaints and disputes to the complainants.	
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives and control effectiveness.	No Exception
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment with regulatory and internal privacy requirements.	No Exception
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception

ART-36	Prior Consultation	CTL14	The organization performs a risk assessment to determine the data types that can be shared with a managed service provider.	Reviewed the Risk Assessment Policy, Vendor Management Policy, and Vendor Risk Assessment Report to verify risk assessments are performed to determine data types shareable with managed service providers.	No Exception
		CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
ART-37	Designation of the data protection officer	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
		CTL5	The organization has established a check-in performance management process for on-going dialogue between managers and employees. (In accordance with the organization-defined frequency) reminders are sent to managers to perform their	Reviewed Performance Reviews and MOM proof of 1-on-1 calendar invites to verify the existence of a scheduled check-in process and	No Exception

			regular check-in conversation.	reminder system for ongoing manager-employee dialogues.	
		CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Reviewed the Change Statement and System Change Policy to verify that change scope, type, roles, workflows, notifications, and approval requirements are pre-defined based on associated risk.	No Exception
ART-38	Position of the data protection officer	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
		CTL5	The organization has established a check-in performance management process for on-going dialogue between managers and employees. (In accordance with the organization-defined frequency) reminders are sent to managers to perform their regular check-in conversation.	Reviewed Performance Reviews and MOM proof of 1-on-1 calendar invites to verify the existence of a scheduled check-in process and reminder system for ongoing manager-employee dialogues.	No Exception

		CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Reviewed the Data Privacy and Retention Policies to verify the existence of a process for addressing privacy inquiries, complaints, and disputes.	No Exception
		CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Reviewed the Data Privacy and Retention Policies to verify mechanisms are in place to address, document, and communicate resolution of privacy complaints and disputes to the complainants.	No Exception
		CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Reviewed the Data Privacy and Retention Policies to verify defined procedures for periodic review and ongoing monitoring of compliance with privacy objectives and control effectiveness.	No Exception
		CTL163	The organization has documented and compiled a report of privacy-related instances of non-compliance with privacy objectives	Reviewed the Data Privacy Policy and Data Retention Policy to verify that the organization has documented privacy-related objectives and established procedures to address non-compliance, ensuring alignment	No Exception

				with regulatory and internal privacy requirements.	
		CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Reviewed the Data Privacy and Retention Policies to verify procedures are disclosed to data subjects for contacting the organization with privacy inquiries, complaints, and disputes.	No Exception
ART-39	Tasks of the data protection officer	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
ART-40	Codes of conduct	CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Reviewed the Organization Chart and Roles Policy to verify key managers are assigned responsibilities to execute the corporate strategy, ensuring organizational alignment.	No Exception
ART-41	Monitoring of approved codes of conduct	CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only	No Exception

				after obtaining implicit or explicit consent.	
ART-44	General principle for transfers	CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
ART-45	Transfers on the basis of an adequacy decision	CTL53	The organization changes shared data encryption keys - at the end of the (organization-defined lifecycle period) - when keys are compromised - upon termination/transfer of employees with access to the keys	Encryption key management aligns with policy, addressing key lifecycle, compromise, and employee access termination	No Exception
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
ART-46	Transfers subject to appropriate safeguards	CTL53	The organization changes shared data encryption keys - at the end of the (organization-defined lifecycle period) - when keys are compromised - upon termination/transfer of employees with access to the keys	Encryption key management aligns with policy, addressing key lifecycle, compromise, and employee access termination	No Exception

		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Reviewed the Data Privacy and Retention Policies to verify that personal information is retained only as long as necessary to fulfill the stated purposes.	No Exception
		CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Reviewed the Data Privacy and Retention Policies to verify defined policies and procedures preventing erasure or destruction of personal information during the specified retention period.	No Exception
		CTL150	The organization has an agreement in place with third parties for disclosure of personal information to those parties.	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify that agreements with third parties include provisions for the disclosure of personal information.	No Exception

		CTL151	The organization has defined a process for assessment of vendors' and other third parties' compliance with personal information disclosure terms, and has defined remedial action in response to the misuse of that personal information	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify defined processes for assessing third-party compliance with personal information disclosure terms and specified remedial actions for misuse.	No Exception
ART-47	Binding corporate rules	CTL150	The organization has an agreement in place with third parties for disclosure of personal information to those parties.	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify that agreements with third parties include provisions for the disclosure of personal information.	No Exception
		CTL151	The organization has defined a process for assessment of vendors' and other third parties' compliance with personal information disclosure terms, and has defined remedial action in response to the misuse of that personal information	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify defined processes for assessing third-party compliance with personal information disclosure terms and specified remedial actions for misuse.	No Exception

		CTL144	The organization has a procedure for communicating privacy policies or other specific instructions or requirements for handling personal information to third parties	Reviewed the Data Privacy and Retention Policies to verify procedures for communicating privacy policies and handling instructions to third parties.	No Exception
ART-48	Transfers or disclosures not authorized by European Union law	CTL144	The organization has a procedure for communicating privacy policies or other specific instructions or requirements for handling personal information to third parties	Reviewed the Data Privacy and Retention Policies to verify procedures for communicating privacy policies and handling instructions to third parties.	No Exception
		CTL145	The organization has a procedure for providing personal information to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject	Reviewed the Data Privacy and Retention Policies to verify procedures ensuring personal information is provided to third parties solely for original purposes and only with implicit or explicit data subject consent.	No Exception
		CTL217	Personal information is disclosed only to third parties who have agreements with The organization to protect personal information in a manner consistent with the relevant aspects of The organization's privacy notice	Reviewed the Data Privacy and Retention Policies to verify that personal information is disclosed only to third parties with agreements ensuring protection consistent with the organization's	No Exception

				privacy notice.	
		CTL217	Personal information is disclosed only to third parties who have agreements with The organization to protect personal information in a manner consistent with the relevant aspects of The organization's privacy notice	Reviewed the Data Privacy and Retention Policies to verify that personal information is disclosed only to third parties with agreements ensuring protection consistent with the organization's privacy notice.	No Exception
ART- 49	Derogations for specific situations	CTL14	The organization performs a risk assessment to determine the data types that can be shared with a managed service provider.	Reviewed the Risk Assessment Policy, Vendor Management Policy, and Vendor Risk Assessment Report to verify risk assessments are performed to determine data types shareable with managed service providers.	No Exception
		CTL129	The organization obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise	Reviewed the Data Privacy Policy to verify that procedures require obtaining explicit consent from data subjects before collecting, using, or disclosing sensitive personal information, unless legally exempt.	No Exception
		CTL130	The organization has defined objectives related to privacy for retaining documentation of explicit consent for the collection, use, or disclosure of sensitive personal	Reviewed the Data Privacy Policy to verify defined objectives for retaining documentation of	No Exception

			information.	explicit consent for sensitive personal information handling.	
		CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Reviewed the Data Privacy Policy to confirm that personal information is used solely for intended purposes and only after obtaining implicit or explicit consent.	No Exception
		CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Reviewed the Data Privacy and Retention Policies to verify that personal information is retained only as long as necessary to fulfill the stated purposes.	No Exception
		CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Reviewed the Data Privacy and Retention Policies to verify defined policies and procedures preventing erasure or destruction of personal information during the specified retention period.	No Exception
		CTL150	The organization has an agreements in place with third parties for disclosure of personal information to those parties	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify that agreements with third parties include provisions	No Exception

				for the disclosure of personal information.	
		CTL151	The organization has defined a process for assessment of vendors' and other third parties' compliance with personal information disclosure terms, and has defined remedial action in response to the misuse of that personal information	Reviewed the Data Privacy and Retention Policies and Vendor Agreement Template to verify defined processes for assessing third-party compliance with personal information disclosure terms and specified remedial actions for misuse.	No Exception