SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: ServiceNow Inc.

EU CLOUD COC

Verification-ID	2022LVL02SCOPE3113
Date of Approval	July 2024
Valid until	July 2025

Table of Contents

1 Verification against v2.11 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.11 (**'v2.11'**)[2] as of December 2020.

Originally drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers – was developed against Directive 95/46/EC[4] and incorporated feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code (v2.11) and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

2 List of declared services

2.1 ServiceNow Platform [6]

The ServiceNow platform is a cloud-based solution that provides a wide range of digital experiences to automate, predict, digitize, and optimize business processes and tasks across the enterprise. It offers a common, highly standardized cloud infrastructure, ensuring the security benefits of customer-specific isolation at the application and database layers.

ServiceNow provides a single product, platform, and support infrastructure, allowing for a large global security team dedicated to securing the Now Platform.

The platform offers a comprehensive security program that covers key physical, administrative, and logical security domains, including architecture, information lifecycle, physical security, security operations, disaster recovery/business continuity, privacy, compliance, and software development 7

The Cloud Service Family (ServiceNow Platform) comprises of the following Cloud Services:

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[6] https://www.servicenow.com/products-by-category.html
[7] NOTE: The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

2.1.1 IT Service Management (ITSM)

Now Assist
Configuration Management Database (CMDB)
Knowledge Management
Incident Management
Change Management
Virtual Agent
Predictive Intelligence
Service Operations Workspace
Now Mobile
Digital Portfolio Management
DevOps Change Visibility
Employee Center
Service Portal
Problem Management
Service Catalog
Asset Management
Workforce Optimization
Process Mining
Contract and Renewal Management
Continual Improvement Management
Site Reliability Operations
DevOps Config
Request Management
Service Level Management

2.1.2 IT Operation Management (ITOM) (STANDARD, PROFESSIONAL, AIOps ENTERPRISE)

Discovery
Service Mapping
Certificate Management
Firewall Audits and Reporting
Service Graph Connectors
Configuration Management Database (CMDB)
Agent Client Collector
Event Management
Metric Intelligence
Health Log Analytics
Cloud Accelerate

2.1.3 HR Service Delivery (HRSD)

Employee Center
Now Assist
Employee Journey Management
Issue Auto Resolution
Case and Knowledge Management
HR Agent Workspace
Now Mobile
Virtual Agent
Universal Request
Performance Analytics
Predictive Intelligence
Process Mining
Employee Relations
Alumni Service Center
Workforce Optimization
Employee Document Management

2.1.4 Workplace Service Delivery (PRO, ENTERPRISE)

Workplace Space Management
Workplace Case Management
Workplace Reservation Management
Workplace Indoor Mapping

Workplace Central

Mobile Wayfinding

Indoor Map Studio

Workplace Move Management

Workplace Visitor Management

Health and Safety

Reporting

Virtual Agent

Now Mobile

Employee Center

Performance Analytics

Workplace Maintenance Management

Workplace Lease Administration

2.1.5 Customer Service Management (CSM)

Self-Service

Workforce Optimization

Process Mining

Now Assist

Virtual Agent

Guided Decisions

Predictive Intelligence

Engagement Messenger

Omnichannel

Workspaces

Case Management

Service Model Foundation

Advanced Work Assignment

Service Management for Issue Resolution

Knowledge Management

Task Intelligence

2.1.6 Field Service Management (STANDARD, PROFESSIONAL)

Now Assist

Schedule Optimization

Field Service Territory Planning

Asset and Cost Management

Process Mining

Workforce Optimization

Dynamic Scheduling

Dispatcher Workspace

Mobile Agent

Planned Maintenance

Virtual Agent

Continual Improvement Management

Predictive Intelligence

Performance Analytics

Field Service Contractor Management

Capacity and Reservations Management

Field Service Crew Operations

Field Service Multi-Day Task Scheduling

Inventory Management

Equipment Scheduling

Task Building

2.1.7 App Engine (App Engine Starter, App Engine)

Now Assist for Creator

App Engine Studio

App Engine Management Center

Studio IDE

Flow Designer

Process Automation Designer

Prebuilt Templates

Delegated Development

2.1.8 Automation Engine (Integration Hub Starter, Automation Engine Professional, Automation Engine Enterprise)

Integration Hub
RPA Hub
Automation Center
Document Intelligence
Stream Connect for Apache Kafka
Process Mining

2.1.9 Strategic Portfolio Management (SPM) (STANDARD, PROFESSIONAL)

Strategic Planning
Scenario Planning
Investment Funding
Agile Development
Scale Agile Framework (SAFe)
Project Portfolio Management
Demand Management
Resource Management
Innovation Management
Digital Portfolio Management
Release Management
Predictive Intelligence
Virtual Agent
Process Mining
Performance Analytics

2.1.10 IT Asset Management (ITAM)

Software Asset Management
Hardware Asset Management
Enterprise Asset Management
SaaS License Management
Asset Management Executive Dashboard
Asset Onboarding and Offboarding
Contract and Renewal Management

2.1.11 Enterprise Asset Management (EAM)

Enterprise Asset Lifecycle Management
Enterprise Asset Estate
Multi-Component Assets
Risk Scoring
Enterprise Asset Inventory
Mobile Asset Receiving
Asset Inventory Audits
Asset Refresh Planning
Enterprise Asset Catalog
Asset Reservations
Recalls
Lease-End Management
Enterprise Asset Maintenance
Enterprise Asset Work Management
Asset Reclamation
Asset Onboarding and Offboarding
Linear Asset Management
Contract and Renewal Management

2.1.12 ServiceNow Vault

ServiceNow Zero Trust Access
Platform Encryption
Data Anonymization
Secrets Management
Log Export Service
Code Signing
Data Discovery

2.1.13 ServiceNow Platform Encryption

Cloud Encryption
Column Level Encryption Enterprise

2.1.14 Security Operations (SecOps)

Security Incident Response
Vulnerability Response
Configuration Compliance
Threat Intelligence Security Center (TISC)
Performance Analytics for Security Operations
Event Management
DLP Incident Response
Major Security Incident Management (MSIM)

2.1.15 Governance, Risk, and Compliance (GRC)

Policy and Compliance Management
Risk Management
Business Continuity Management
Third-party Risk Management
Operational Risk Management
Continuous Authorization and Monitoring
Operational Resilience Management
Privacy Management
Regulatory Change Management
Audit Management
Use Case Accelerators
Performance Analytics
Virtual Agent
Predictive Intelligence

2.1.16 Third-Party Risk Management

Onboarding, offboarding, and renewals due diligence
Third-party portal
Risk intelligence and ongoing monitoring
Concentration risk map
Third-party portfolio management
Third-party risk management workspace
Issue management and remediation
Aggregated risk scores

2.1.17 Telecommunications Service Operations Management

Event Management
Operational Intelligence
TM Forum Open APIs

2.1.18 Operational Technology Management

OT Foundation

OT Visibility

OT Vulnerability Response

OT Service Management

2.1.19 ServiceNow Cloud Observability

Notebooks

OpenTelemetry

Correlation Engine

Unified Query Language (UQL)

Cloud-Native Logging

Intelligent Alerts

Unified Dashboards

OpenTelemetry Service Management

2.1.20 Telecommunications Network Inventory

Network Inventory Data Model

Equipment Models and Templates

Design and Assign

VLAN or LAG Number Management

Cable and Fiber Strand Management

Network Inventory Configurable Workspace

2.1.21 Clinical Device Management

HL7 FHIR Data Model

Device Visibility

Planned Work Management

Alternate Equipment Maintenance

Device In-Service

Issue Reporting

Advanced Risk Assessment

2.1.22 Employee Growth and Development

Employee Center Pro

Manager Hub

2.1.23 Health and Safety

Employee Center

Health and Safety Incident Management

Workplace Case Management

Contact Tracing

Safe Workload Dashboard

Vaccination Status

Employee Travel Safety

Employee Health Screening

Health and Safety Testing

Workplace PPE Inventory Management

Employee Readiness Surveys

2.1.24 Legal Service Delivery

Legal Investigations

Legal Request Management

Legal Counsel Center

Legal Matter Management

Legal Contracts

Reporting

Legal Knowledge Management

Employee Center

Now Mobile

Mobile Agent

Virtual Agent

2.1.25 Sourcing and Procurement Operations (SPO)

Procurement Case Management

Shopping Hub

Now Mobile

Employee Center

Knowledge Management

Reporting

2.1.26 Supplier Lifecycle Operations

Knowledge Management

Performance Analytics

Procurement Case Management

Third-party Risk Management

Now Mobile

2.1.27 Financial Services Operations

Personal and Commercial Lines Servicing for Insurance

Deposit Operations for Banking

Financial Services Data Model

Financial Services Card Operations

Financial Services Payment Operations

Financial Services Loan Operations

Performance Analytics

Financial Services Document Management

Workspaces

Case and Knowledge Management

Omni-Channel

Advanced Work Assignment

Predictive Intelligence

Self-Service

Virtual Agent

Knowledge Management

Communities

Visual Task Assignment

Customer Central

Playbook for Customer Service

Guided Decisions

Visual Workflow and Automation

Mobile Agent

Walk-Up Experience

Proactive Customer Service Operations

Problem Management

Customer Project Management

2.1.28 Telecommunications Service Management

Service Bridge

Telecommunications Assurance Workflows

Order Management for Telecommunications

Workspaces

Case Management

Omni-Channel

Customer Central
Advanced Work Assignment
Playbooks for Customer Service
Guided Decisions
Predictive Intelligence
Self-Service
Virtual Agent
Knowledge Management
Communities
Flow Designer
Proactive Customer Service Operations
Problem Management
Visual Task Boards
Mobile Agent
Performance Analytics
Reporting
Surveys and Assessments
Continual Improvement Management
TM Forum APIs
Catalog Versioning
Horizontal Catalog Dependencies

2.1.29 Order Management

Product Bundles and Attributes
Product Detail Pages
Self-Service
Agent Order Capture
Product Catalog
Order Capture API
Price Lists

2.1.30 Order Management for Technology Providers

Product Catalog and Data Model
Product and Service Agnostic
Order Capture API
Dynamic Orchestration Plans

2.1.31 Order Management for Telecommunications

Order Management for Telecommunications
Fallout Management
In-Flight Order Changes
Attribute Propagation
TM Forum APIs
Order Capture
Staggered Decomposition
Process Mining

2.1.32 Technology Provider Service Management

Omni-Channel
Integrated Self-Service
Virtual Agent
Predictive Intelligence
Service Bridge
Technology Service Workflows
Playbooks for Customer Service
Proactive Customer Service Operations
Proactive Customer Engagement
Guided Decisions
Advanced Work Assignment
Service-Aware CMDB

Workspaces
Customer Central
Reports and Dashboards
Case and Knowledge Management
Performance Analytics
Workforce Optimization

2.1.33 Healthcare and Life Sciences Service Management

Vaccine Administration Management
Pre-Visit Management
Patient Support Services
Patient 360
Digital Documentation
Consent Management
Workspaces
Omni-Channel
Self-Service
Virtual Agent
Knowledge Management
Communities
Playbooks for Customer Service
Guided Decisions
Predictive Intelligence
Performance Analytics
Case Management
Visual Task Boards
Surveys and Assessments

2.1.34 Public Sector Digital Services

Public Sector Data Model
Government Services Portal
Workspaces
Engagement Messenger
Virtual Agent
Predictive Intelligence
Performance Analytics
Playbooks for Customer Service
Guided Decisions
Walk-Up Experience
Request Management
Omni-Channel
Customer Central
Advanced Work Assignment
Self-Service

2.1.35 Accounts Payable Operations

Now Mobile
Third-party Risk Management
Procurement Case Management
Document Intelligence
Knowledge Management

2.1.36 Integration Hub[8]

Out-of-the-Box Spokes[9]

Custom Spokes[9]

Flow Templates

Packaged Integration Solutions

Integration Hub Import

Spoke Generator[9]

REST API Trigger

Remote Tables

Connections Dashboard

Stream Connect for Apache and Kafka

2.1.37 Manufacturing Connected Workforce

App Engine Studio

Now Mobile

Workspaces

Visual Task Boards

Flow Designer

3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[10].

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba[11].

The Code has been officially approved in May 2021[12]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[13]. The robust and complex procedures and mechanisms can be reviewed by any third-party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[14]

[8] **NOTE:** Subject to the Code is the connectivity feature, i.e., the integration subject to appropriate technical and organisational measures. Not in scope of this declaration of adherence is any of the services that might be integrated by the Customer respectively the processing activities of such services. The listing in this report shall only reflect the capabilities at the time of assessment.

[9] **Provided by the CSP:** Definitions: A Spoke is a predefined action, flow, and/or integration for connecting or automating third party systems or processes within Flow Designer.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[11] https://scope-europe.eu

[12] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf

[13] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf

[14] https://eucoc.cloud/en/public-register/assessment-procedure/

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set out by the supervisory authority pursuant to Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; proactively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

3.3 Multiple Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e., continuous, rigorous, and independent monitoring, an independent complaints' handling process, and finally any CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Controls Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications, their respective reports and by free text responses. Additionally, the CSP will have to provide a general overview of the functionalities, technical, organisational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognised standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third-party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g., by sample-taking and requesting further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided that over a due period every Control will be subject to scrutiny by the Monitoring Body. Where applicable, aspects of current attention at the time of assessment shall be covered too, e.g., where such aspects were indicated in media reports, publications or actions of supervisory authorities.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indicating appropriate implementation by the Control Guidance, then, the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon, makes them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.11 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is, however, no difference in terms of which parts of the Code are covered, since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the “First Level of Compliance”, Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body’s report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms of providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third-party certificates and audit reports, that are recognised by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

Identical to the “Second Level of Compliance” but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognised standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is at the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[15] and referring to the Public Register of the EU Cloud CoC[16] to enable Customers to verify the validity of adherence.

4 Assessment of declared services by ServiceNow (see 2.)

4.1 Fact Finding

Following the declaration of adherence of ServiceNow Inc. ('**ServiceNow**'), the Monitoring Body provided ServiceNow with a template, requesting ServiceNow to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal[17], the Monitoring Body requested from ServiceNow a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from ServiceNow a comparison of the declared Cloud Services of last year and this year as well as to explicitly indicate any Cloud Services that are no longer included in the Declaration of Adherence and, where applicable, provide the Monitoring Body with adequate reasons. To the extent the list of Cloud Services was extended, the Monitoring Body requested a confirmation, that any such additional Cloud Services are subject to the same technical, organisational and contractual framework as the original Cloud Services.

ServiceNow promptly responded to the templates. Information provided consisted of references and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable. This information was completed by the confirmations requested by the Monitoring Body as well as a detailed comparison of the declared Cloud Services between last year and this year verification highlighting the changes and the reasons for them.

[15] https://eucoc.cloud/en/public-register/levels-of-compliance/

[16] https://eucoc.cloud/en/public-register/

[17] You can access the Verification Report of the previous year via the following link: ServiceNow Verification Report (2023)

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[18], the Monitoring Body analysed the responses and information provided by ServiceNow.

ServiceNow's declared services have been externally certified and audited. ServiceNow holds an ISO 27001, which is valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services. The declaration of adherence referred to the respective ISO 27001 certification within the responses to Section 6 of the Code (IT Security). As provided by the Code, the Monitoring Body may consider third-party certifications and audits. Accordingly, the Monitoring Body verified the certification and references. Further in-depth checks were not performed, as provided third-party certifications adequately indicated compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from ServiceNow which outlined how all the requirements of the Code were met by ServiceNow's implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of Controls from the Code for in-depth scrutiny. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information. The Controls selected for this level of review were: 5.1.A, 5.1.D-E, 5.1.H, 5.2.D-G, 5.3.D-E, 5.4.A, 5.5.A, 5.5.C, 5.5.E-F, 5.7.D-F, 5.8.A-B, 5.12.A-B, 5.12.D, 5.12.G, 5.13.B, 5.14.F, 6.1.D, 6.2.I and 6.2.P.

4.3.2 Findings by the Monitoring Body

During the process of verification, ServiceNow consistently prepared the Declaration of Adherence well and thoroughly. ServiceNow's responses were detailed and never created any impression of intentional non-transparency. Requests for clarification, additional and supporting information, as well as relevant samples were promptly dealt with and always met the deadlines set by the Monitoring Body.

[18] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

Related to the Monitoring Body's requests (see section 4.1), ServiceNow indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual framework. Where additional Cloud Services were added, ServiceNow provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

The monitoring Body has focused on the Customers' Audit Rights, including inspections. ServiceNow has provided the information that most recent third-party audit reports and certifications are provided to the Customers via dedicated self-service portal. Customers may then reach out to the ServiceNow for additional information and support. Further, Customer Audit rights are included as a part of the contractual documentation and ServiceNow indicated to allow and contribute for Customer-requested audits, including on-site inspections. ServiceNow has affirmed that costs associated with Customer-requested audits are communicated to the Customers and that such audits are cost neutral.

The assistance and information provided to the Customers have been in the scope of the assessment. It has been indicated by ServiceNow that Cloud Service Agreement incorporating the data protection obligations under GDPR as a minimum, is in place with the Customers. ServiceNow makes relevant information including product documentation and instructions available via self-service platform. Additional assistance is available to the Customers and may be requested via dedicated communication channels. In this regard, ServiceNow identified that Customers are provided with self-service capabilities to maintain data retention policies and schedules, covering data deletion, retrieval and export of Customer Personal Data in machine readable, commonly used, structured format.

Another area of the assessment was built around Code adherence communication. ServiceNow has indicated that Adherence to the Code is transparently communicated to the Customers via dedicated communication channels and to its personnel, enabling to adequately deal internally with related Customer inquiries.

When it comes to the subprocessor management, ServiceNow indicates that contractual documents define information on the processing activities in relation to Customer Personal Data engaged by suprocessors, including the lists of the subprocessors with relevant general information. Additionally, the subprocessor management program is in place to ensure that the same data protection obligations and appropriate technical and organisational measures, as provided to the Customers, are flown down throughout the full subprocessing chain.

The Monitoring Body has assessed the data breach notification and reporting obligations. ServiceNow has indicates that security and incident management policies and procedures are implemented. The data breach reporting obligations and Customer notification are included in the contractual documents with Customers and relevant internal policies and procedures ensures the appropriate identification and handling of the data breaches, in case such breaches happen.

Third country transfers have been assessed by the Monitoring Body, ServiceNow confirmed to implement the relevant data transfer safeguards as provided by Chapter V GDPR such as adequacy decisions and Standard Contractual Clauses ('SCCs'). The adequacy decision monitoring is implemented alongside with the regional legislative changes and data privacy requirements review process.

Another area of the assessment was records of processing activities ('ROPA'). Based on the information provided by ServiceNow, it maintains ROPA in its capacity as Processor, which includes the relevant information as per Article 30.2 GDPR. The Customers are provided with a possibility to provide and update the information in relation to the completion and relevancy of the ROPA, as a part of the available self-service capabilities.

5 Conclusion

The information provided by ServiceNow were consistent. Where necessary, ServiceNow gave additional information or clarified their given information appropriately.

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 1. The service(s) will be listed in the Public Register of the EU Cloud CoC[19] alongside this report.

In accordance with sections 3.4.1.2and 3.4.2 and given the type of information provided by ServiceNow to support the compliance of its service, the Monitoring Body grants ServiceNow with a Second Level of Compliance.

6 Validity

This verification is valid for one year. The full report consists of 22 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[20].

[19] https://eucoc.cloud/en/public-register/

[20] https://eucoc.cloud/en/public-register/

Verification-date: July 2024 **Valid until**: July 2025

Verification-ID: 2022LVL02SCOPE3113