

RECORD OF PERSONAL DATA PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 OF REGULATION (EU) 2018/1725

SERVICENOW as IT Service Management Tool (ITSM)

Contents

General information.....	1
Description and Purpose of the Processing	2
Data Subject’s Rights.....	3
Categories of Data Subjects & Personal Data	4
Categories of Recipients & Data Transfers.....	5
Automated Decision Making	7
Retention Period & Security Measures.....	7

General information

Introduction
EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) No 2018/1725 (further referred as the Regulation) ¹ .
Contact Details of Data Controller(s)
Fausto Parente, Executive Director Westhafenplatz 1, 60327 Frankfurt am Main, Germany fausto.parente@eiopa.europa.eu
Contact Details of the Data Protection Officer
Eleni Karatza Westhafenplatz 1, 60327 Frankfurt am Main, Germany dpo@eiopa.europa.eu
Contact Details of Processor

¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

EIOPA's Team/Unit/Department responsible for the processing: Information Technology Unit - Corporate Support Department
Contact Details of External Processor(s) / Joint Controller(s)
<input checked="" type="checkbox"/> External processor(s): ServiceNow, Nederland B.V. Hoekenrode 3, 1102 BR, Amsterdam, Zuidoost, The Netherlands ServiceNow Luchthaven Brussel Nationaal 1K, Zaventem, Brussels 1930, Belgium CANCOM Public BV, Rue Montoyer 25 Brussels, 1000 Brussels European Securities and Markets Authority (ESMA), 201-203 Rue de Bercy, 75012 Paris, France <input type="checkbox"/> Joint controller(s): <input type="checkbox"/> N/A

Description and Purpose of the Processing

Description of Processing
<p>The purpose of the ITSM tool is to enhance efficiency and effectiveness of the IT Help Desk in managing incidents tickets, problems and change request of EIOPA IT infrastructure and applications. In particular, it serves as a platform for submitting and tracking incidents, problems, and errors reported by EIOPA internal and external stakeholders. Additional services may be added in the future. The ITSM tool is provided by ServiceNow.</p> <p>As part of IT support and service delivery, EIOPA collects and uses personal data for the following purposes:</p> <ul style="list-style-type: none">• communicate incidents, requests, security events and warnings relating to IT operations, applications, and services;• respond and contain raised IT requests, security events and incidents;• provide support and facilitate IT operations;• increase the awareness of staff in the field of cyber security and IT best practices;• facilitate dialog with internal and external EIOPA service providers;• monitor, detect and prevent incidents and problems using IT systems;• production of statistics concerning IT service requests, incidents, problems and IT infrastructure changes to drive performance improvements.
Purpose (s) of the processing

<input type="checkbox"/> Staff administration <input checked="" type="checkbox"/> Relations with external parties <input type="checkbox"/> Procurement and accounting <input type="checkbox"/> Administration of membership records <input checked="" type="checkbox"/> Auditing <input checked="" type="checkbox"/> Information administration <input type="checkbox"/> Other (please give details):
Lawfulness of Processing
<ul style="list-style-type: none">• Legal Basis justifying the processing: EIOPA's founding Regulation (EU) No 1094/2010• Processing is necessary: <input checked="" type="checkbox"/> for the performance of a task carried out in the public interest <input type="checkbox"/> for compliance with a legal obligation to which the Controller is subject <input type="checkbox"/> for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract <input type="checkbox"/> in order to protect the vital interests of the data subject or of another natural person Or <input type="checkbox"/> Data subject has given his/her unambiguous, free, specific and informed consent

Data Subject's Rights

Information on how to exercise data subject's rights
Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018. Data subjects have the right to: <ul style="list-style-type: none">• access their personal data, receive a copy of them in a structured and machine-readable format or have them directly transmitted to another controller, as well as request their rectification or update in case they are not accurate.• request the erasure of their personal data, as well as object to or obtain the restriction of their processing.• withdraw their consent to the processing of their personal data at any time in case such processing is based solely on their consent. For the protection of the data subjects' privacy and security, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion.

Should data subjects wish to access/rectify/delete their personal data, or receive a copy of them/have it transmitted to another controller, or object to/restrict their processing, please contact IT-DPC@eiopa.europa.eu or DPO@eiopa.europa.eu.

Complaint:

Any complaint concerning the processing of the data subjects' personal data can be addressed to EIOPA's Data Protection Officer (DPO@eiopa.europa.eu). Alternatively, data subjects can also have at any time recourse to the European Data Protection Supervisor (www.edps.europa.eu).

Categories of Data Subjects & Personal Data

Categories of Data Subjects

- EIOPA permanent staff, Temporary or Contract Agents
- SNEs or trainees
- Visitors to EIOPA (BOS, MB, WG, Seminars, Events, other)
If selected, please specify:
- Providers of good or services
- Complainants, correspondents and enquirers
- Relatives and associates of data subjects
- Other (please specify): Member State National Competent Authorities staff

Categories of personal data

(a) General personal data:

The personal data contains:

- Personal details (name, address etc)
- Education & Training details
- Employment details
- Financial details
- Family, lifestyle and social circumstances
- Other (please give details): email address, work location, work phone

(b) Special categories of personal data

The personal data reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs

<input type="checkbox"/> Trade union membership <input type="checkbox"/> Genetic or Biometric data <input type="checkbox"/> Data concerning health, sex life or sexual orientation
--

Categories of Recipients & Data Transfers

Recipient(s) of the data
<input type="checkbox"/> Managers of data subjects <input checked="" type="checkbox"/> Designated EIOPA staff members If selected, please specify: EIOPA IT Unit members participating in troubleshooting, incidents resolution, service requests or change requests. <input type="checkbox"/> Relatives or others associated with data subjects <input type="checkbox"/> Current, past or prospective employers <input type="checkbox"/> Healthcare practitioners <input type="checkbox"/> Education/training establishments <input type="checkbox"/> Financial organisations <input checked="" type="checkbox"/> External contractor: - ServiceNow and its subprocessors. The full list of ServiceNow general subscription sub-processors can be found here. - Other IT service providers participating in the service delivery, incident resolution or change implementation: e.g. ATOS, CANCOM, OTE, that could therefore have secondarily access to the personal data collected. <input type="checkbox"/> Other (please specify):
Data transfer(s)
<input type="checkbox"/> Within EIOPA or to other EU Institutions/Agencies/Bodies If selected, please specify: <input checked="" type="checkbox"/> To other recipients within the EU : A. ServiceNow ServiceNow servers are located within the EU (Dublin, Amsterdam and Germany). B. The other service providers mentioned above <input type="checkbox"/> To third countries If selected, please specify: Whether suitable safeguards have been adopted:

- Adequacy Decision of the European Commission²
- Standard Contractual Clauses (SCC)
- Binding Corporate Rules (BCR)
- Administrative Arrangements between public Authorities (AA)

A. Service Now

The service is provided through ServiceNow’s Protected Platform for costumers in the European Union (SPP EU). ARTASK0026081.

By default, all data, including User-Generated Information, created by users when they use ServiceNow, is stored in ServiceNow’s data centres within the EEA.

The exceptions to the SPP EU contractual commitment to not transfer EU-hosted personal data out of the EU are limited to the following:

- Where non-EU access has been approved by the customer in advance.³
- Where required to prevent or remediate a material issue involving security, data loss, prevention, disaster recovery or critical maintenance/service availability.⁴
- Where required by law or to prevent fraud or abuse.⁵
- Where data is documented in a Support Portal interaction (by or on behalf of the customer), provided that ServiceNow personnel accessing such interactions are located in the EU. Note that Customers can control what data they put or request to be put in the Support Portal.

In the case of exceptions mentioned above, ServiceNow has put safeguards in place such as Standard Contractual Clauses and technical and organisational measures. More information on the appropriate safeguards used by ServiceNow can be found [here](#).

B. The other service providers mentioned above have also implemented appropriate safeguards, where necessary.

To international organisations

If selected, please specify the organisation and whether suitable safeguards have been adopted:

² Third countries for which the European Commission has issued adequacy decisions are the following: [Adequacy decisions \(europa.eu\)](#)

³ For example, a scenario where a customer grants an exception directly in relation to a particular function, such as wanting to work with particular ServiceNow personnel based outside of the EU for a specific reason.

⁴ Examples of where this exception may apply include but are not limited to: EU support center is down and cannot correspond with Customers; EU datacenter is down, and extra staff is needed to support incoming cases; national network outage; ServiceNow network component is down for the EU.

⁵ It may be possible that ServiceNow could be involved in litigation with a customer or related party that mandates certain data disclosures, or ServiceNow could also become aware of fraud / payment avoidance / systems manipulation / targeted attacks / other illegal activity, in which case ServiceNow would need to reserve the right to have any necessary access to Customer data to prevent or remediate such issues.

Automated Decision Making

Automated Decision-making, including profiling
A decision is taken in the context of this processing operation solely on the basis of automated means or profiling: <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes In case of an automated decision-making or profiling, please explain:

Retention Period & Security Measures

Retention period
Service requests and incidents including the personal data of the requester are kept for 3 years from the date of the service or incident being requested, to allow for the effective and coherent handling of recurrent requests and the production of statistics concerning EIOPA services.
For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised: <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes
Technical & organisational security measures taken
Several technical and organisational measures have been adopted in order to ensure the optimum security of the documents and personal data collected in the context of the procedures described under section 'Description and Purpose of the Processing'.
Security of Processing – detailed analysis
A cloud computing solution (Cloud-based SaaS) is used. Information on ServiceNow's security measures can be found here . • Technical & Organisational Security measures adopted: <input checked="" type="checkbox"/> Controlled access to ICT-system/controlled access codes <input checked="" type="checkbox"/> Restricted access to physical location where data is stored <input type="checkbox"/> Pseudonymisation and Encryption <input checked="" type="checkbox"/> Back-up <input checked="" type="checkbox"/> Audit trails (wrt ServiceNow)

<input checked="" type="checkbox"/> Confidentiality agreement/clause
<input type="checkbox"/> Test the effectiveness of security measures adopted
<input type="checkbox"/> Training of staff
<input type="checkbox"/> Other (please specify):