

connect.
engage.
succeed.

Connecting to Privacy Workspace
External documentation
29-7-2019



Document data

Publication data	
Title	Connecting to Privacy Workspace – external documentation
Version	1.5
Date	16-12-2020
Author	Eddy van de Werken
Department	Integrated Solutions
Company name	Centric Netherlands B.V.

Contact details	
Contact	Eddy van de Werken
Telephone	+31 6 14 49 54 13
Email	Eddy.van.de.werken@centric.eu
Web Page	https://www.centric.eu/NL/Default/Privacy-Workspace

Contact details history		
1.0	First release	25-6-2018
1.1	Update of category to array string	9-7-2018
1.2	Removed status concept	14-8-2018
1.3	Corrected typo in PrivacyLogDTO description	29-7-2019
1.4	Changed category from array to multi-value field	8-12-2020
1.5	Added create table statements	16-12-2020

Copyright 2018, Centric Netherlands B.V.

No part of this publication may be reproduced, stored in a retrieval system or disclosed in any form or by any means, whether electronically, mechanically, by photocopying, recording or otherwise, without written permission of Centric Netherlands B.V.

Table of Contents

Document data 2

1 Introduction 4

2 What needs to be done? 5

1 Introduction

In order to enable the data controllers to obtain privacy logging information of different applications of multiple suppliers (as part of GDPR measurements), this document describes the technical structure for applications to produce privacy logging information that can be processed by Centric's Privacy Workspace.

2 What needs to be done?

In order to connect towards Privacy Workspace there are a number of steps that need to be done:

1. All codes mentioned below need to be negotiated with Centric's product manager, Eddy.van.de.Werken@centric.eu

Application related information	AppCode Name Purpose
Process related information (for each individual process per application)	ProcessCode Name Purpose Description
Action related information (for each individual action per application)	ActionCode Name Description
Subject (unique value equal for all applications)	SubjectTypeCode Name Description
Object (unique value equal for all applications)	ObjectTypeCode Name Description

2. Privacy logging information needs to be written in a database (Microsoft SQL or Oracle) in a so called Data Transfer Object (DTO). This object requires the connecting applications to push their logs in a standardized way towards Privacy Workspace.

Name	Type	R/O	Definition
Id	Number	R	Unique identifier of the logging record
Version	String	R	Version number of the PrivacyLogDTO
PrivacyLogDTO	String	R	JSON string containing the PrivacyLogDTO
State	String	R	State of the message which can contain the values NOT SEND, SENDING and RECEIVED. This state is used to delete the successfully received messages from the queue The default value is NOT SEND
OrganizationCode	String	O	Unique identifier for an organization

R/O: Required or Optional

The Privacy logging queue is the database table where the log data from on premise (Centric) applications is stored. This table is added to the current database schema of an application or in a separate database schema. The name of this database(schema) can be determined by Centric or the customer.

Dependent on the connecting application this will be a Microsoft SQL database/table or an Oracle database/table. Both definitions of the privacy log table are stated in the next sub-sections. Be aware that the OrganizationCode is omitted because this is an optional field that is only needed in multi-tenant and multi-municipality situations.

Microsoft SQL Server

```
-- Create schema
if NOT EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE
TABLE_SCHEMA = 'loggingAgent')
BEGIN
    EXEC sp_executesql N'CREATE SCHEMA loggingAgent'
END
```

```
-- Create Privacylogs table
if NOT EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE
TABLE_NAME = 'PAA_PRIVACYLOGS' AND TABLE_SCHEMA =
'loggingAgent')
BEGIN
    CREATE TABLE [loggingAgent].[PAA_PRIVACYLOGS] (
        MESSAGE_ID UNIQUEIDENTIFIER DEFAULT NEWID() NOT NULL,
        MESSAGE_VERSION [VARCHAR](20) NOT NULL,
        MESSAGE_JSON [VARCHAR](MAX) NOT NULL,
        MESSAGE_STATE [VARCHAR](10) DEFAULT('NOT SEND') NOT NULL,
        CONSTRAINT [PK_PAA_PRIVACYLOGS] PRIMARY KEY CLUSTERED
        (
            [MESSAGE_ID] ASC
        ) WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
        IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS =
        ON) ON [PRIMARY]
    ) ON [PRIMARY];

    ALTER TABLE [loggingAgent].[PAA_PRIVACYLOGS]
    ADD CONSTRAINT [PAA_C_STAT]
    CHECK ( MESSAGE_STATE in (
        'NOT SEND',
        'SENDING',
        'RECEIVED'
    ));
END;
```

Oracle RDBMS

```
-- Create table
create table PAA_PRIVACYLOGS
(
    message_id RAW(16) not null,
    message_version VARCHAR2(20) not null,
    message_json CLOB not null,
    message_state VARCHAR2(10) not null
)
;
-- Create/Recreate check constraints
alter table PAA_PRIVACYLOGS
add constraint PAA_C_STAT
check (message_state in ('NOT SEND','SENDING','RECEIVED'));
```

3. The PrivacyLogDTO requires the following data elements

Name	Type	R/O
organization	String	R
appCode	String	R
appLogVersion	String	R
processCode	String	R
actionCode	String	R
accessorId	String	R
accessorName	String	R
accessorRole	String	R
accessorAuthorization	String	O
objectTypeCode	String	O
objectId	String	O
subjectTypeCode	String	R
subjectId	String	R
purposeLimitation	String	O
category	String*	O
dataSource	String	O
logDateUtc	DateTime	R
remark	String	O

R/O: Required or Optional

*category can be a comma separated multi-value field (see example)

Message with example data:

```
{
  "organization": "Mun001",
  "appCode": "App x",
  "appLogVersion": "2.4.1",
  "processCode": "P001",
  "actionCode": "A001",
  "accessorId": "Ex@mpl&!D",
  "accessorName": "Naam Verwerker",
  "accessorRole": "Beheerder",
  "accessorAuthorization": "Active Directory",
  "objectTypeCode": "OT0001",
  "objectId": "Obj&ct!D",
  "subjectTypeCode": "BSN",
  "subjectId": "000000000",
  "purposeLimitation": "Agreement",
  "category": "Financial data, Personal data",
  "dataSource": "Database app x",
  "logDateUtc": "2018-06-22T14:30:08.4714372Z",
  "remark": "Additionele opmerking"
}
```

4. Building the log triggers in the application

To actually start with writing log records towards a privacy logging table according to the DTO format it is necessary to implement triggers in the application. These triggers must be built in at the screens, business layer and links with other components of the application.

5. Fill the privacy log table

After the triggers are implemented, the privacy log table will be filled with a log entry after each event in the application that is related to the processing of personal data. This privacy log table can be added in the current database schema of the application or in a separate schema.