



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Security Deployment Guide

Genesys Engage cloud Support for GDPR

Contents

- 1 Genesys Engage cloud Support for GDPR
 - 1.1 Process for Genesys Engage cloud
 - 1.2 JSON File Format
 - 1.3 Customer Expectations & Assumptions

Genesys Engage cloud Support for GDPR

This page provides information that is specific to the Genesys Engage cloud implementation of support for General Data Protection Regulation (GDPR). For general information about Genesys support for GDPR, see [General Data Protection Regulation \(GDPR\)](#).

Important

In general, Genesys support for GDPR compliance is based on default configuration settings and typical application usage. Other underlying components within Genesys Engage cloud do not store sensitive information beyond 30 days.

Genesys has a standard JSON format for both Right of Erasure (Forget Me) and Right of Access and Portability (Export).

Process for Genesys Engage cloud

- Open a support case using the Customer Care portal.
- Select the Case Sub Type of Data Privacy.
- Provide the input JSON file. This JSON file will contain information on what action is required to be taken and will also include the consumer-identifying input for GDPR requests (forget me and/or export).
- Customer Care can assist in creating the JSON files that will form the input for the Export or Delete request. Customers can also create these JSON files. See [JSON Format](#) for a sample format.
- Genesys will then process the JSON files to fulfill the request.
- After the file is processed, Customer Care will post the execution log or exported records to the SFTP site in the Case (Under Transfer Files).
- The customer can validate the execution log and based on the response messages, a follow-up action may be required. If the execution was not successful, a corrected request may be resubmitted.

Notes for Outbound

- The *shortcodes* array in the request is used only to execute searches for the mobile channel (SMS/MMS). You can skip it or provide an empty array.
- If shared shortcodes are specified in the request, they will not be included in the exported result.
- The *accountid* is created during the provisioning process and is required for Outbound. PEC Care can obtain this value for each tenant if it is not already known.

Notes for Portico Aggregation or Mobile Messaging Manager (MMM)

- The *shortcodes* array in each JSON request is mandatory for these products since they are exclusively used for mobile messaging (SMS/MMS).
- If shared shortcodes are specified in the request, they will not be included in the exported result.
- The *accountid* parameter can be ignored.

JSON File Format

Genesys has a standard JSON format for both Right of Erasure (Forget Me) and Right of Access and Portability (Export).

Input JSON File Naming Conventions

Customers create a plain-text JSON file using the following pattern: **<request_type>-<date:yyyyMMdd>_<uniqueID_or_timestamp>.json** where

- **<request_type>** is either *forget* or *export*.
- **<date:yyyyMMdd>** allows for limited pickup of files placed on the directory structure by date. Automated processing will occur on files matching the current date only.
- **<uniqueID_or_timestamp>** to ensure filenames are unique within a day. Files with the exact same name should not be posted to the pickup location.

Example file name: **forget-20180315_120000.json** OR **export-20180315_120000.json**

Submit File Content

The following sample can be used as a starting template. It models a request for 2 different GDPR compliance requests. This request format can be pasted into a tool like <https://jsoneditoronline.org/> to visualize and edit within the structure. It is beyond the scope of these directions to cover a description of the JSON structure or suggest any tools that can be used to help create or edit JSON.

- requests - An array of one or more request objects. At least one is required.
- requestcase - (Optional and not processed) Used to match requests with results. This can be used to store a ticket case number or internal identifier.
- shortcodes - An array of shortcodes used for SMS activity. If SMS channel is not used, submit an empty array.
- accountid - A string containing the account number to search within the Engage platform. This can be an enterprise account number which will search all accounts in an enterprise.
- type - "FORGET" or "EXPORT" are the only supported values. All requests in the payload should have the same type and should match the file name prefix.
- contacts - An array of device type and value pairings. Specify as many or as few as specified by the end user. Allowable device types within the contacts array: phone, email, ipaddr:
 - phone - must be in ITU E.123 international format: like +1 781 555 1212

- email - must follow standard email conventions (include 1 "@" and no less than 1 dot in domain portion, no illegal characters in username)
- ipaddr - likely to be supplied in IPv4 format (4 sets of numbers with 3 dots between)

```
{
  "requests": [{
    "requestcase": "97456596893834",
    "shortcodes": ["11111", "22222"],
    "accountid": "30003748347",
    "type": "FORGET",
    "contacts": [{
      "phone": "+1 781 555 1212"
    },
    {
      "phone": "+1 617 555 1212"
    },
    {
      "email": "test@test.com"
    },
    {
      "email": "genesys@genesys.com"
    },
    {
      "ipaddr": "10.10.10.10"
    },
    {
      "ipaddr": "11.11.11.11"
    }
  ]
},
{
  "requestcase": "6457657657",
  "shortcodes": ["11111", "22222"],
  "accountid": "30003748347",
  "type": "FORGET",
  "contacts": [{
    "phone": "+1 781 555 1313"
  },
  {
    "phone": "617 555 1313"
  },
  {
    "email": "test2@test.com"
  },
  {
    "email": "genesys2@genesys.com"
  },
  {
    "ipaddr": "10.10.10.11"
  },
  {
    "ipaddr": "11.11.11.12"
  }
]
}
]
```

Submit File Location

Properly named files shall be posted to a directory named **GDPR_Submit** on the supplied SFTP

account. Only files placed in this specifically named directory will be processed.

Delete/Export Result Format and Retrieval

Result File Retrieval Location

A properly named and submitted file will generate a result file for DELETE or EXPORT requests. All result files will be found in a directory on the same SFTP account named **GDPR_Result**.

Result File Naming

Result files will have the exact same name as submitted files except a suffix will be appended:
-execution-log

Example result file name format: *forget-20180315_120000-execution-log.json* OR
export-20180315_120000-execution-log.json

Result File Content: Execution Log

Result files contain the original request array. The result array is appended and follows the same format as the original request with the inclusion of a new property named "response" within each "contacts" object. The string value for "response" will always either be "SUCCESS" or "ERROR" followed by some additional explanation for the error. It is important to note that any errors found apply only to processing for that contact device. This means that a request against other contacts will not be stopped because of the failure for one. The expected action simply will not have been completed for the error device: Not deleted in the case of "forget" requests and is not provided in any result content for "export" requests. Any "ERROR" devices will need to be corrected and resubmitted.

Both "SUCCESS" and "ERROR" responses include support for an additional reason message. All "ERROR" responses will include this additional reason. "SUCCESS" responses will include a "not found" message if the device did not return results.

```
{
  "requests": [{
    "requestcase": "97456596893834",
    "shortcodes": ["11111", "22222"],
    "accountid": "30003748347",
    "type": "FORGET",
    "contacts": [{
      "phone": "+1 781 555 1212"
    },
    {
      "phone": "+1 617 555 1212"
    },
    {
      "email": "test@test.com"
    },
    {
      "email": "genesys@genesys.com"
    },
    {
      "ipaddr": "10.10.10.10"
    },
    {
      "ipaddr": "11.11.11.11"
    }
  ]
}
```

```
    }
  ]
},
{
  "requestcase": "6457657657",
  "shortcodes": ["11111", "22222"],
  "accountid": "30003748347",
  "type": "FORGET",
  "contacts": [{
    "phone": "+1 781 555 1313"
  },
  {
    "phone": "617 555 1313"
  },
  {
    "email": "test2@test.com"
  },
  {
    "email": "genesys2@genesys.com"
  },
  {
    "ipaddr": "10.10.10.11"
  },
  {
    "ipaddr": "11.11.11.12"
  }
  ]
},
],
"result": [{
  "requestcase": "97456596893834",
  "shortcodes": ["11111", "22222"],
  "accountid": "30003748347",
  "type": "FORGET",
  "contacts": [{
    "phone": "+1 781 555 1212",
    "response": "SUCCESS"
  },
  {
    "phone": "+1 617 555 1212",
    "response": "SUCCESS"
  },
  {
    "email": "test@test.com",
    "response": "SUCCESS"
  },
  {
    "email": "genesys@genesys.com",
    "response": "SUCCESS"
  },
  {
    "ipaddr": "10.10.10.10",
    "response": "SUCCESS"
  },
  {
    "ipaddr": "11.11.11.11",
    "response": "SUCCESS"
  }
  ]
},
{
  "requestcase": "6457657657",
  "shortcodes": ["11111", "22222"],
```

```
"accountid": "30003748347",
"type": "FORGET",
"contacts": [{
  "phone": "+1 781 555 1313",
  "response": "SUCCESS"
},
{
  "phone": "617 555 1313",
  "response": "ERROR: incorrect device format"
},
{
  "email": "test2@test.com",
  "response": "SUCCESS"
},
{
  "email": "genesys2@genesys.com",
  "response": "SUCCESS"
},
{
  "ipaddr": "10.10.10.11",
  "response": "SUCCESS"
},
{
  "ipaddr": "11.11.11.12",
  "response": "SUCCESS"
}
]
}
```

Result File Content: Export Results

Export results will have the exact same name as submitted files except a "-archive" suffix will be appended and the results will be bundled in a .zip archive. Example name: export-20180315_120000-archive.zip

Any exported data that is derived from a list (active contact records or historical contact attempt records) will be exported as plaintext, comma-delimited CSV.

Export result archives WILL NOT include call recordings (though they are in scope for FORGET requests). To extract call recordings, customers should run one or both of the Script Recording or Client Recording reports via the Account Manager's "Reports" tab.

Customer Expectations & Assumptions

For "forget" or "export" requests, customers are expected to:

- Limit the set of "request initiators" to a small, qualified set of resources.
- Ensure a consumer's requested devices are accurately provided. By transposing a digit in a phone device, a "forget" request for an unintended consumer could be initiated OR possibly worse, "export" results for the wrong party could be produced which, if not reviewed before distribution, are a breach of privacy. Any processed "forget" requests will result in irreversible anonymisation for their devices, if found.

- Ensure expected execution-log files are received. Depending on number of requests in the posted payload, more than 1 execution-log may result. If no results are found, correct posted file names.
- Check execution-log files for error messages for any provided device and repost any corrected files as needed to completely satisfy their consumer's request.
 - For "forget" requests, translate execution-log results into a consumable confirmation to their consumers, if needed.
 - For "export" requests, review, filter, or transform archive results to ensure that only results for the intended consumer(s) are provided.
- Refrain from posting their consumer's GDPR requests or results to forums or portals (whether Genesys-provided or not) as doing so perpetuates PII on other platforms.
- Remove a consumer's data from future files posted to Genesys platforms. GDPR requests will result in a one-time removal as of that point in time and do NOT result in additions to device or clientID suppression/DNC. If suppression is additionally desired as a "safety check," customers already have UI or API methods to take that action.

Important

A "forget" request will result in an entity in scope (historical contact attempt record, list record, etc.) to be no longer searchable by device. This is because found devices are turned into unrecognizable placeholder equivalents. For this reason, the only way to confirm "forget" behavior after processing a request is to submit an "export" request or do a contact trace/search by ClientID to confirm that fields with PII have been redacted.