
Archiefvernietigingscomponent

Release 0.1.0

Maykin Media

Apr 25, 2021

INDEX

1	Getting started	3
1.1	Introduction	3
1.1.1	Integration tips for software suppliers	3
1.1.2	Who's behind the Archiefvernietigingscomponent?	5
1.1.3	Open-source	5
1.2	Installation	5
1.2.1	Quickstart installation	5
1.2.2	Configuration	6
1.2.3	Demo mode	14
1.2.4	Deployment	15
1.3	Manual	17
1.3.1	Roles	17
1.3.2	Destruction process overview	17
1.3.3	Step by step process (Dutch)	21
1.3.4	Frequently asked questions	22

The **Archiefvernietigingscomponent** (Archive destruction component) for “Zaakgericht werken” (case-oriented working) allows you to destroy case information, documents and decisions, as dictated by the Dutch law.

GETTING STARTED

To get you started, you might find some of these links relevant:

- New to the application? Have a look at the [Introduction](#)
- How to use the application? Read the [Manual](#)
- Want to get started quickly? Follow the [Quickstart installation](#)
- Ready to install the application? Head over to [Deployment](#).
- How to deal with local/domain data in other applications? Check out the [Integration tips for software suppliers](#).

1.1 Introduction

Record management is the practice of destroying data-records that have met their end-of-life time. “Zaakgericht werken” prescribes the archiving terms for cases that have been brought to an end.

The Archiefvernietigingscomponent (AVC) provides functionality for record managers to schedule destruction of cases according to the archiving parameters. It implements a multi-step, multi-role accordance process.

Attention is paid to the user experience of the staff using the app, with notifications to inform you of pending workload, full audit logging and traceability of user and system actions.

The AVC supports all backends implementing the 1.0.x [API's voor Zaakgericht Werken](#), like [Open Zaak](#). It is designed according to [Common Ground](#) principles as a re-usable application.

1.1.1 Integration tips for software suppliers

The Archiefvernietigingscomponent destroys cases, related documents and decisions in the [API's voor Zaakgericht Werken](#). The application has no direct control over data that is stored in other applications, registers, APIs or components.

It's the responsibility of the record manager or archivist to make sure that data, related to the case that is deleted, is also deleted. There are some technical considerations that can be made to delete related data automatically when the case is deleted.

Software suppliers can make use of the implementation scenarios below to facilitate the destruction process in accordance with the Dutch law.

Implementation scenarios

In all cases, your application needs to store the case identifier (URL or UUID) that links the local data with the case in the [Zaken API](#) in order to match them.

Subscribe to the Notifications API

When a case is deleted, a notification is sent to all subscribers by the [Notifications API](#). This behaviour is part of the [API's voor Zaakgericht Werken](#) and not specific for the Archiefvernietigingscomponent.

Your application can listen to these notifications and delete its locally stored data that is related to the case that is deleted.

Keep in mind that when you receive the notification, the case is already deleted and it can no longer be retrieved from the Zaken API.

Keep track of the “archieffactiedatum”

Although this is not good [Common Ground](#) practice, your application can make a copy of the `archieffactiedatum` of the case and store it with your local data.

You can then schedule regular intervals to update your copy of the `archieffactiedatum` in case it changes and schedule a regular destruction process to delete your local data according to the (locally kept) `archieffactiedatum`.

This destruction process should check if the case is already deleted. Cases are typically not deleted on, or right after, their `archieffactiedatum` and local data should not be deleted before the case is deleted!

Keep track of deleted cases

A more simple version of the above but less efficient and more prone to issues.

Your application can check whether a case is deleted in the [Zaken API](#). Although you cannot really check if a case is deleted, you can only check if the case is not present (anymore) in the [Zaken API](#).

This might be a trigger to delete your local data as well. You should however be very careful with situations where there is another reason why you cannot retrieve a case from the [Zaken API](#) anymore (authorizations, network issues, URL changes, etc.)

Storing local/domain data in an (third party) API

If your application stores data in an (third party) API, like the [Objects API](#), it is still the responsibility of your application to delete the objects in such an API. The object needs to have (and thus store) a relation to the case in order to match it to the deleted case.

You can then use one of the implementation scenarios to perform the deletion.

1.1.2 Who's behind the Archiefvernietigingscomponent?

Initially, the Archiefvernietigingscomponent was called the Record Management App and was created by the municipality of Utrecht. Later, it was picked up by several municipalities to iterate on the work to create a re-usable application. In alphabetical order, they are:

- Delft
- Haarlem
- Rotterdam
- Tilburg
- Utrecht

The municipality of Utrecht and Delft take the lead in this project and the application is developed by [Maykin Media](#) under the [Open Gemeente Initiatief](#).

1.1.3 Open-source

The Archiefvernietigingscomponent is open-source and available under the [EUPL license](#).

In addition, this project makes use of various open-source [Python libraries](#) and [npm packages](#) under the hood.

1.2 Installation

1.2.1 Quickstart installation

A `docker-compose-quickstart.yml` file is available to get the app up and running in minutes. It contains 'convenience' settings, which means that no additional configuration is needed to run the app. Therefore, it should *not* be used for anything else than testing. For example, it includes:

- A default `SECRET_KEY` environment variable
- A predefined database with the environment variable `POSTGRES_HOST_AUTH_METHOD=trust`. This lets us connect to the database without using a password.
- Debug mode is enabled.

Getting started with Docker

1. Download the `docker-compose` file:

Linux

Windows (Powershell 3)

```
$ wget https://raw.githubusercontent.com/maykinmedia/
↪archiefvernietigingscomponent/master/docker-compose-quickstart.yml -O docker-
↪compose.yml
```

```
PS> wget https://raw.githubusercontent.com/maykinmedia/
↪archiefvernietigingscomponent/master/docker-compose-quickstart.yml -Odocker-
↪compose.yml
```

2. Start the docker containers with `docker-compose`. If you want to run the containers in the background, add the `-d` flag to the command below.

```
$ docker-compose up
```

3. Create a super-user.

```
$ docker-compose exec web src/manage.py createsuperuser
```

Defaults

Warning: Loading the default roles could overwrite existing user accounts.

1. Load the default roles, email contents and review answers:

Docker

Python

```
$ docker-compose exec web src/manage.py loaddata default_roles default_
↪emails default_review_answers
```

```
$ source env/bin/activate
$ python src/manage.py loaddata default_roles default_emails default_
↪review_answers
```

To learn more about the roles, emails and review answers, go [here](#), [here](#) and [here](#) respectively.

2. Navigate to `http://127.0.0.1:8000` and use the credentials created above to log in.

If you want to enable the demo mode, continue to [Demo mode](#). You can also start [configuring](#) the application if you have no need for the demo mode.

1.2.2 Configuration

Quickstart

This is the minimal configuration and assumes you loaded in the default roles described in the [Defaults](#). You can also define your own roles as described in the [More configuration](#).

Services

The Archiefvernietigingscomponent must be connected to an instance of Open Zaak.

1. Navigate to the Archiefvernietigingscomponent admin.
2. Configure the credentials for the Zaken API (so the Archiefvernietigingscomponent can access the Zaken API):
 - a. Navigate to **API Autorisaties > Services**
 - b. Click **Service toevoegen**.
 - c. Fill out the form:

- **Label:** Open Zaak – Zaken API
 - **Type:** Select the option: ZRC (Zaken)
 - **API root url:** *For example:* `http://example.com/zaken/api/v1/`
 - **Client ID:** *For example:* `avc-demo`
 - **Secret:** *Some random string. You will need this later on!*
 - **Authorization type:** Select the option: ZGW client_id + secret
 - **OAS:** URL that points to the OAS, same URL as the *API root url* with `/schema/openapi.yaml` added to it *for example:* `https://example.com/api/v1/schema/openapi.yaml`
 - **User ID:** *Same as the Client ID*
 - **User representation:** *For example:* `Archiefvernietigingscomponent`
- d. Click **Opslaan**.
3. Repeat the steps above for the **Catalogi API** and the **Documenten API**. Make sure to use the same Client ID and Secret for each of them.

For the **Catalogi API**, also fill in **Extra configuration** with:

```
{"main_catalogus_uuid": "<the UUID of your main catalog>"}
```

4. Add the Selectielijst API:
- a. Navigate to **API Autorisaties > Services**
 - b. Click **Service toevoegen**.
 - c. Fill out the form:
 - **Label:** Open Zaak (public) – Selectielijst API
 - **Type:** Select the option: ORC (Overige)
 - **API root url:** `https://selectielijst.openzaak.nl/api/v1/`
 - **Authorization type:** Select the option: No authorization
 - **OAS:** `https://selectielijst.openzaak.nl/api/v1/schema/openapi.yaml`
 - d. Click **Opslaan**.

Open Zaak

1. Navigate to the Open Zaak admin.
2. Configure the credentials for the Archiefvernietigingscomponent (so the Archiefvernietigingscomponent can access the various Open Zaak APIs):
 - a. Navigate to **API Autorisaties > Applicaties**
 - b. Click **Applicatie toevoegen**.
 - c. Fill out the form:
 - **Label:** Archiefvernietigingscomponent
 - **Heeft alle autorisaties:** *Checked*
 - **Client ID:** *The same as configured in the Archiefvernietigingscomponent.*

- **Secret:** *The same as configured in the Archiefvernietigingscomponent.*
- d. Click **Opslaan**.

More configuration

Note: This part of the configuration documentation is aimed at (functional) administrators.

The Archiefvernietigingscomponent supports run-time configuration for maximum flexibility to make it fit your environment. This does also mean that a fresh installation is empty and not useful without any configuration.

The configuration interface is available on <https://example.com/admin/>, where `example.com` should be replaced by your actual domain.

Accounts, roles and permissions

Permissions

The Archiefvernietigingscomponent has a simple permission system, consisting of the following permissions:

can start destruction

Someone who can start destruction is allowed to create destruction lists. A person with this permission will see a list of their own destruction lists on their landing page, and a button to create a new list.

can review destruction

Someone with this permission can be assigned as a reviewer for a destruction list. On their landing page, they see an overview of all the destruction lists where they were once assigned as a reviewer. They can suggest changes/exemptions on destruction lists back to the destruction list author.

can view case details

Someone with this permission is allowed to view more details about a case. This could be part of the review process or destruction list creation process.

Roles

Navigate to **Authenticatie en autorisatie > Rollen** to manage roles. Roles define a set of permissions. An application user can have one role.

Typical example roles would be:

- **record manager:**
 - *can start destruction:* yes
 - *can review destruction:* no
 - *can view case details:* yes
- **process owner:**
 - *can start destruction:* no
 - *can review destruction:* yes
 - *can view case details:* yes

- **archivist:**
 - *can start destruction:* no
 - *can review destruction:* yes
 - *can view case details:* no

You can create as many roles as you want and name them as you see fit.

There is a fixture to load default roles.

Docker

Python

```
$ docker-compose exec web src/manage.py loaddata default_roles
```

```
$ source env/bin/activate
$ python src/manage.py loaddata default_roles
```

This adds 4 *Roles* in the application: process owner, archivist, record manager and functional administrator. Process owner, archivist and record manager are described [here](#), while the functional administrator is a role with all the permissions of the three roles above combined.

Accounts

Via **Authenticatie en autorisatie > Gebruikers** you can manage individual users known to the system. You can perform administrative actions such as:

- assigning a role to a user
- filling out their name/e-mail address
- (re)setting their password

ADFS

The Archiefvernietigingscomponent admin interface and frontend support logging in through ADFS-backed single sign on (SSO).

ADFS 2012 and 2016, and Azure AD are supported. See the [ADFS config guides](#) for documentation on how to configure ADFS itself.

The ADFS configuration can be found under **Admin > Configuration > ADFS Configuration**.

Services

The Archiefvernietigingscomponent does not store, synchronize or copy case data. All data is retrieved through the Zaken, Catalogi and Documenten API. As such, these services need to be configured.

Navigate to **Configuratie > Services** and add the details for your environment.

Note: Archiefvernietigingscomponent supports multiple services of the same type.

Catalogi API

The Archiefvernietigingscomponent uses the Catalogi API to provide filter options based on “zaaktype”.

Add a service of the type ZTC, and make sure to fill out:

- `API root URL`: the API base URL of the service.
- `Extra configuration`: a JSON object with the main catalogue ID, e.g.:

```
{ "main_catalogus_uuid": "09a4ae7a-98a3-4178-9559-b22b76cad3db" }
```

- `Client ID`: the client ID for your “application” that was registered with the Catalogi API-serving application.
- `Secret`: the Secret for your “application” that was registered with the Catalogi API-serving application.
- `Authorization type`: ZGW-client_id + secret
- `OAS`: URL to the API schema, normally this is `API root URL + schema/openapi.yaml`.
- `NLX url`: optional NLX outway-URL if the service is to be consumed over the NLX network.

Zaken API

The Zaken API is used to retrieve the zaken matching the archiving terms. They are the objects that are eventually destroyed by this application.

Add a service of the type ZRC. The configuration steps for the Catalogi API apply here, with the exception of “Extra configuration” - this is not required.

Documenten API

Cases (“zaken”) almost always have relations to documents. If the case is being destroyed, documents related to it (and no other cases) also need to be destroyed. For that purpose, the Archiefvernietigingscomponent needs access to the Documents API.

Add a service of the type DRC. The configuration steps for the Catalogi API apply here, with the exception of “Extra configuration” - this is not required.

Selectielijst API

The steps to configure a service to a Selectielijst API are the same as those for the Documenten API, except that the type of service is ORC.

Why is the Selectielijst API needed?

When a list is destroyed, a report of destruction is generated with references to all the cases that were destroyed. This report contains the following fields:

1. `Unieke kenmerk`: the `identificatie` field of a case
2. `Beschrijving`: the `omschrijving` field of a case
3. `Looptijd`: the number of days between the `enddatum` and `startdatum` field of a zaak.
4. `Vernietigings-Categorie selectielijst`: the `nummer` field of the `selectielijstProcestype` of the `zaaktype`.
5. `Toelichting`: the name of the destruction list

6. **Opmerkingen:** the comment in the latest approval review from the archivaris (user with a role with permissions to review the destruction, but not to start the destruction or view case details).
7. **Reactie zorgdrager:** the comment in the latest approval review from the process eigenaar (user with a role with permissions to review the destruction and review case details, but not to start the destruction).

In order to retrieve the data for point 4., a service to a Selectielijst API needs to be configured. Otherwise this field will be left empty in the report.

Required scopes

The Catalogi, Zaken and Documenten API enforce authorization checks. For the correct functioning of the Archiefvernietigingscomponent, it needs the following scopes:

Zaken API

- `zaken.lezen`: used to display detail information
- `zaken.geforceerd-bijwerken`: used to change archiving parameters for exemptions
- `zaken.verwijderen`: used to destroy selected cases

Catalogi API

- `catalogi.lezen`: used to fetch available case-types

Documenten API

- `documenten.lezen`: used to display case detail information
- `documenten.verwijderen`: used to destroy documents as part of the case destruction

Besluiten API

- `besluiten.lezen`: used to display case detail information
- `besluiten.verwijderen`: used to delete “besluiten” as part of the case destruction

Archive configuration

The Archiefvernietigingscomponent only offers cases of which the archive action date has passed, to prevent destruction of cases before their scheduled archiving. This is annoying for testing purposes, so the Archiefvernietigingscomponent supports specifying the “current date”.

Navigate to **Configuratie > Archiveringsconfiguratie** to specify the “current date”.

Theme settings

You can easily change the colors, logo and footer texts to match the ones from your organization.

Navigate to **Configuration > Thema configuratie** to configure the theme.

Setting the domain

In the admin, under **Configuratie > Websites**, make sure to change the existing *Site* to the domain under which the Archiefvernietigingscomponent will be deployed.

Automatic emails

The system administrator can decide to configure automatic emails to be sent to the reviewers and/or the record manager. This can be done through the admin, under **Configuratie > Automatische emails**

If there are already automatic emails present, they can be edited. There are three types of automatic emails:

- Review required: for when a reviewer has a destruction list to review.
- Changes required: for when a record manager needs to process the feedback form a reviewer.
- Report available: for when a destruction report is sent to the archivist.

A custom email subject and email body can be configured for each type of email. If no automatic emails are present in the admin in **Configuratie > Automatische emails**, then no emails will be sent.

To load default automatic emails, a fixture is present. This can be loaded with the following command (from the `archiefvernietigingscomponent/` directory):

Docker

Python

```
$ docker-compose exec web src/manage.py loaddata default_emails
```

```
$ source env/bin/activate
$ python src/manage.py loaddata default_emails
```

A few variables can be used in the email body. These are:

- `{{ user }}`: it will be replaced with the full name (first name and last name) of the user receiving the email.
- `{{ municipality }}`: it will be replaced with the name of the municipality sending the email.
- `{{ list }}`: it will be replaced with the name of the destruction list.
- `{{ link_list }}`: it will be replaced with the link to the destruction list.
- `{{ link_report }}`: it will be replaced with the link to where the PDF of the destruction report can be downloaded.

Note: In order to use the variable `{{ municipality }}`, the municipality name needs to be configured under **Configuratie > Email configuratie**.

Note: The variable `{{ link_report }}` can only be used in the email of type “Report available”.

Standard review answers

When a reviewer asks for changes to a destruction list, they can choose from a drop down the reason why they are asking for changes. These reasons can be configured in the admin under **Reviews > Standard review antwoorden** and then **Standard review antwoorden toevoegen**. Both the text and the order in which these reasons will appear in the dropdown can be configured. Once you have added multiple reasons in the admin, you can use the up and down arrows on the right (see screenshot below) to change the order.

Selecteer standaard review antwoorden om te wijzigen

Actie: Uitvoeren 0 van de 10 geselecteerd

REDEN	MOVE
☐ Zaken die van belang zijn voor de huidige bedrijfsvoering/nog andere lopende zaken.	⌵ ⌴ ⌵ ⌴
☐ Zaken die bij een vastgestelde Hotspot behoren.	⌵ ⌴ ⌵ ⌴
☐ Zaken met een uniek karakter.	⌵ ⌴ ⌵ ⌴
☐ Bijzondere gebeurtenissen.	⌵ ⌴ ⌵ ⌴
☐ Beeldbepalende, karakteristieke, bijzondere objecten.	⌵ ⌴ ⌵ ⌴
☐ Samenvattingen van gegevens.	⌵ ⌴ ⌵ ⌴
☐ Belangrijke burgers en functionarissen.	⌵ ⌴ ⌵ ⌴
☐ Bescheiden die vervangen wat door een calamiteit verloren is gegaan.	⌵ ⌴ ⌵ ⌴
☐ Precedenten: individuele zaken die leiden tot algemene regels.	⌵ ⌴ ⌵ ⌴
☐ Bescheiden waarbij de vernietiging de logische samenhang zou verstoren.	⌵ ⌴ ⌵ ⌴

10 standaard review antwoorden

To load in default reasons, the fixture `default_review_answers` can be loaded as follows:

Docker

Python

```
$ docker-compose exec web src/manage.py loaddata default_review_answers
```

```
$ source env/bin/activate
$ python src/manage.py loaddata default_review_answers
```

This feature will load the following reasons (in this order):

- Zaken die van belang zijn voor de huidige bedrijfsvoering/nog andere lopende zaken.
- Zaken die bij een vastgestelde Hotspot behoren.
- Zaken met een uniek karakter.
- Bijzondere gebeurtenissen.
- Beeldbepalende, karakteristieke, bijzondere objecten.
- Samenvattingen van gegevens.
- Belangrijke burgers en functionarissen.
- Bescheiden die vervangen wat door een calamiteit verloren is gegaan.
- Precedenten: individuele zaken die leiden tot algemene regels.
- Bescheiden waarbij de vernietiging de logische samenhang zou verstoren.

Audit trails

In version 1.0, the templates used for the audit trail have been renamed. Their extension was changed from `.txt` to `.html`. A management command was added to change the template name in all existing logs. This can be executed as follows:

Docker

Python

```
$ docker-compose exec web src/manage.py convert_log_templates
```

```
$ source env/bin/activate
$ python src/manage.py convert_log_templates
```

1.2.3 Demo mode

The demo mode is meant to guide you through the application, following a predefined process with predefined roles.

Warning: Do not use this mode in production or any publicly accessible environment. In doing so, you might expose case data, documents, etc.

Prerequisites

You will need:

- A working Archiefvernietigingscomponent, for example as installed via the [Quickstart installation](#),
- Full access to all [API's voor Zaakgericht werken](#), like an [Open Zaak](#) instance,
- Access to a Selectielijst API, like: <https://selectielijst.openzaak.nl>.

Note: We assume you are using Open Zaak but this can be an component that offers the [API's voor Zaakgericht werken](#).

Setting up demo mode

1. Enable demo mode.

The demo mode can be activated by setting the environment variable `AVC_DEMO_MODE` to 1. By default `AVC_DEMO_MODE=0`.

Docker

Python

Change the `docker-compose.yml` file you are using to include the environment variable:

```
web:
  image: maykinmedia/archiefvernietigingscomponent:latest
  environment: &web_env
    - AVC_DEMO_MODE=1
```

(continues on next page)

(continued from previous page)

```
- DJANGO_SETTINGS_MODULE=archiefvernietigingscomponent.conf.docker
# etc...
```

and stop and start the docker containers (do not just restart).

```
$ docker-compose down
$ docker-compose up -d
```

```
$ AVC_DEMO_MODE=1 python src/manage.py runserver
```

2. Navigate to `http://127.0.0.1:8000` and you will see that demo mode is enabled.
3. Click the red **Administration** button and login to start configuring the application.
4. For testing purposes we can fake the current date. Normally, only cases that should be destroyed today or earlier show up. If we set the date to 50 years in the future, most cases will show up.
 - a. Navigate to **Configuratie > Archiveringsconfiguratie**
 - b. Fill in the **Archiefdatum** to specify the fake “current date”.
 - c. Click **Opslaan**.

Note: When the record-management app is in demo mode, cases are not *actually* destroyed, i.e. they remain in OpenZaak and can be included in new destruction lists.

You can continue to *configure* the application.

1.2.4 Deployment

Deployment is done via [Ansible](#). Currently, only single server deployments are described but you can just as easily deploy the application in a Kubernetes environment.

Warning: The deployment configuration (called a “playbook”) is very simplistic and also contains sensitive values. This makes the playbook more readable but is not following good practices!

Server preparation

You can configure the Ansible playbook to install relevant services, do it manually, or have these pre-installed. You will need:

- PostgreSQL
- Nginx
- Docker
- Python3
- Python3 PIP

Apart from Docker, you can install all these with something like:

```
$ sudo apt-get install postgresql nginx python3 python3-pip
```

For Docker, follow the instructions here: <https://docs.docker.com/engine/install/>

You will also need access to, or create, a database. You can create a database with something like:

```
$ sudo su postgres --command="createuser <db-username> -P"
Enter password for new role:
Enter it again:
$ sudo su postgres --command="createdb <db-name> --owner=<db-username>"
```

Installation

1. Download the project from Github or just the [deployment files](#).

```
$ git clone git@github.com:maykinmedia/archiefvernietigingscomponent.git
```

2. Setup virtual environment:

```
$ python3 -m venv env/
$ source env/bin/activate
$ pip install ansible
```

Note: Sometimes, additional or updates packages are needed if they are not installed by the Ansible setup installation. You can do so like this:

```
$ python -m pip install -U pip
$ pip install ordered_set packaging appdirs six
```

3. Install Ansible collections:

```
$ ansible-galaxy collection install community.docker
$ ansible-galaxy collection install git+https://github.com/maykinmedia/
↪commonground-ansible.git
```

Note: The last collection might require explicit access.

4. Edit the playbook `app.yml` to match your setup. Take special note of all **TODO** settings and **read through all the comments and variables**.
5. Run the playbook:

```
$ ansible-playbook app.yml --become --ask-become-pass
```

1.3 Manual

The Archiefvernietigingscomponent has typical roles and with these roles, one can follow a certain destruction process.

1.3.1 Roles

Typically the Archiefvernietigingscomponent has 3 roles but you can rename these roles in the application or create roles with different permissions.

Record manager

- The record manager initiates the process to destroy cases and generates the list of destruction.
- Executes quality control over the list, checks if there are relations that can't be disconnected when the file is destroyed and if there are cases on the list that can't be destroyed because of an exemption due to the criteria mentioned in the 'selectielijst' (this is the archiving policy list with all the storage periods per zaaktype/process and allowed exemptions).
- Makes sure the destruction list is forwarded to the process owner.

Process owner

- As the owner of the information, checks if all the cases on the list can be destroyed. Asks the question: Is the file still needed for the current business operation?
- Exempts files that are still needed and gives the argumentation for that.
- Approves the list, so it can be forwarded (in extracted form/proces verbaal) to the municipal archivist/supervisor. Or sends the list back to the record manager, if there are exceptions/exemptions.
- Approves (after the approval of the municipal archivist and the actual destruction) the proces verbaal.

Municipal archivist / supervisor

- Checks the request/proces verbaal from the process owner.
- Rejects or gives approval for the destruction.

1.3.2 Destruction process overview

The destruction process takes care of destroying the case data, with respect to their archiving law parameters.

As part of "zaakgericht werken" ("case management"), the archive parameters are determined during the life-cycle of a case. There are two possible actions:

- destroy cases
- keep cases (and transfer them to an e-depot)

Each case has an "archive action date", which is the date after which the determined action needs to be performed.

The derivation of these parameters is part of the standard for "API's voor Zaakgericht Werken". The Archiefvernietigingscomponent provides the tooling to perform the destruction of the cases past the archive action date.

Note: When we mention destruction, we mean permanent destruction. The API calls made to the involved API's cause the data to be erased from the database and documents to be removed from the file systems.

The next sections document the process as implemented in the Archiefvernietigingscomponent.

Destruction list creation

A user with sufficient permissions (see *Accounts, roles and permissions*) can bring up the destruction list creation screen.

Filters are provided on the left hand side, while the main content shows a table of cases matching the filter criteria. Only the cases that have their archive action date before or on the current date are available.

Filters

The filters allow you to select a sub-set of cases based on case-type. Each case type displays the various versions, so you can limit the selection to a specific version.

You can also filter on start date - only cases started before or on the selected date are retrieved.

Case selection

The destruction list author adds cases to the destruction list by checking the checkbox. The checkbox in the table heading can be used to toggle *all* cases matching the provided filters.

In the top-right, a summary of the amount of selected cases is displayed.

Finalizing the list creation

Once all relevant cases have been selected, the list author can now finalize the list creation by clicking the top-right button, which brings up a form.

The form requires you to give the list a name for identification purposes, and you specify which users should be involved in the review process. The reviewers should be selected in order of review.

Available users are selected based on their role permission.

There is also a checkbox which can be used to specify whether the destruction list contains cases with sensitive information. If the checkbox is checked (default), the report of destruction will *NOT* contain the case description and the remarks of the archivist.

Once the confirmation button is clicked, the list is created and assigned to the first reviewer.

Lists overview

In the start page, the record manager has an overview of all the lists that they created. To facilitate searching through the lists, there are filters on the left-hand side:

- In progress (*In behandeling*): lists that are waiting to be reviewed and lists that have been approved, but are waiting to be processed.
- Action required (*Actie vereist*): lists that have been reviewed, but not approved. The reviewer may either have asked for changes or rejected them.
- Completed (*Verwerkt*): lists that have been processed and the cases have been deleted.
- All (*Alle*): All lists.

Destruction list review

Each reviewer assigned to a list performs the review in turn after the previous reviewer has approved the destruction list.

Reviewers with *process owner* role have the option to suggest exemptions or changes:

- exemptions: suggests removing the case from the destruction list
- changes: the reviewer can provide a comment so that the author knows which changes to make to the archiving parameters. The case will also be removed from the list

Once a reviewer suggests changes or exemptions, the original list author is assigned, where they process the changes. After processing the changes, the review flow restarts with the first reviewer.

If the author of the destruction list disagrees with changes suggested in a review, they can add a comment before submitting the list for further review. Only the reviewer who created the controversial review will be able to see the comment.

Reviewers with *archivist* role do NOT have the option to suggest changes or exemptions, but they can reject a list in its entirety. After an archivist has rejected a list, the original list author is assigned. The author can then decide whether to abort the list and start a new one, make changes to the existing list, or simply add a comment for the archivist explaining why they disagree with their review.

After the last reviewer has given their approval, the list is submitted for actual destruction to the background worker queue.

After destruction

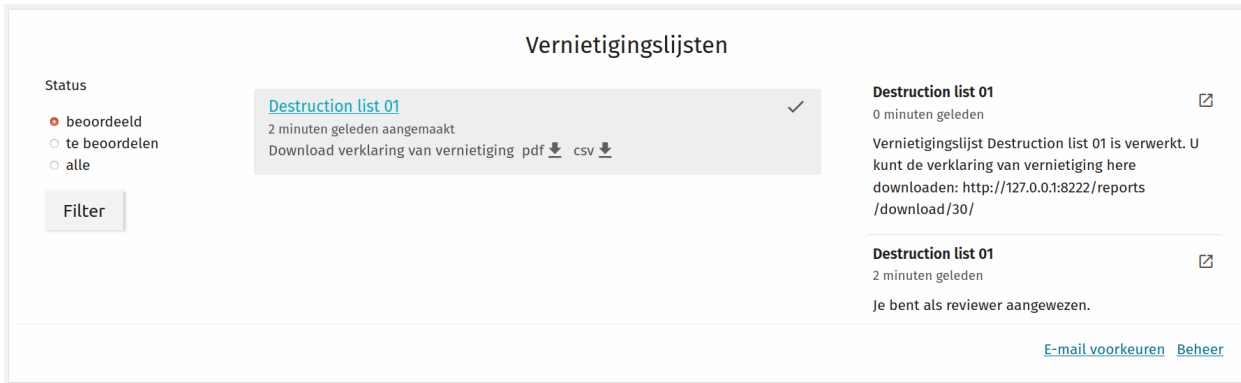
Once a list has been destroyed, a report of destruction is created. The report contains the following information:

- Uniek kenmerk
- Beschrijving *
- Loop tijd
- VCS
- Toelichting
- Opmerkingen *
- Reactie Zorgdrager
- Zaaktype

- Bewaartermijn
- Resultaatype
- Verantwoordelijke organisatie
- Relaties

The fields with asterisk are optional. They are only present if the record manager unchecked the checkbox `Contains sensitive details` when they created the destruction list.

The destruction report is generated both as a PDF and a CSV file. It contains the information mentioned above for each case that was destroyed. The link to the report is sent via email to the archivist who reviewed the list and the process owner can download the report within the AVC app. The link can be found in the page with path `vernietigen/reviews/` after filtering for lists that have already been reviewed. All lists with an associated report will have a link (see image below).



In addition, the PDF of the destruction report contains the audit trail of the destruction process. It shows in chronological order which actions have been performed and the role of the user who performed the action.

Audit trails, logs and notifications

Audit trails are collected for list creation, review submission and case deletion (for every individual case!).

In addition, destruction list assignees receive notifications within the app when important events happen, such as being the next assignee on the list or when a destruction report is ready.

If configured, automatic emails can also be sent to notify the reviewers and/or the record manager when there is work that needs their attention. There are three types of automatic emails that can be configured:

- An email for the reviewer for when a destruction list needs to be reviewed.
- An email for the record manager for when there are changes requested by a reviewer.
- An email for the archivist with as attachment a report of destruction.

Each user can also update their email preferences. They can decide whether to receive an email as soon as there is work waiting for them or to never receive emails. The link to the page where email preferences can be changed is at the bottom right of the entry view.

Deleting a list

Should the author decide to cancel the destruction process for a list of cases, they can use the ‘abort’ button in the top right hand corner of the list details page. Clicking this button will cancel only the list, i.e. the cases will *NOT* be destroyed. The cases that were part of the cancelled list will become available again to be included in other destruction lists.

1.3.3 Step by step process (Dutch)

Note: This section is in Dutch and follows the same steps as the *Demo mode*.

Hieronder staat een typische workflow door het vernietigingsproces zoals dat mogelijk wordt gemaakt met deze applicatie. Het is mogelijk om het proces iets anders in te richten met behoudt van dezelfde functionaliteiten. Deze globale functionaliteiten staan beschreven in *Destruction process overview*.

Recordmanager

Taak: Opstellen vernietigingslijst (VL)**

Doel: Het initiëren van de vernietiging van verzamelingen zaken die wettelijk vernietigd moeten worden.

1. Kies **Opstellen**. Alle zaken die in aanmerking komen voor vernietigen worden opgehaald.
2. Verfijn je selectie indien gewenst met de opties onder **Filters** door specifieke zaaktypen aan te vinken, of door de minimale datum waarop vernietigd mag worden mee te geven.
3. Selecteer nu onder **Zaakdossiers** de zaken die je op de VL wilt zetten. Wanneer je Zaaktype aanvinkt, worden alle zaken in de lijst aangevinkt. Je kunt desgewenst afzonderlijke zaken af- en aanvinken.
4. Na selectie van de zaken, kies je voor **Aanmaken**.
5. Er verschijnt een dialoogvenster **Vernietigingslijst starten**, waarin wordt opgegeven:
 - **Naam:** De naam van de VL
 - **Eerste reviewer:** De proces eigenaar (selecteer in de pulldown `demo-proces-eigenaar@example.com`)
 - **Tweede reviewer:** De archivaris (selecteer in de pulldown `demo-archivaris@example.com`).

Kies **Bevestig**.

6. Je ziet de VL nu in het overzicht van lijsten die door gebruiker record manager zijn aangemaakt. Met een icoontje wordt aangegeven dat de lijst onderhanden is.
7. Wanneer er aanpassingen zijn voorgesteld door een proces eigenaar op eerder opgestelde lijsten, zie je deze lijsten ook terug in dit overzicht.

Log nu in als process eigenaar om de VL beoordelen.

Processowner

Taak: Beoordelen vernietigingslijst (VL)

Doel: Het controleren van de juistheid van verzamelingen zaken die volgens de record manager vernietigd moeten worden. Aan de hand van de controle kunnen suggesties worden doorgegeven aan de record manager.

Je ziet nu het overzicht van VLen. Je kunt het overzicht aanpassen naar de status (beoordeeld, te beoordelen, alle). Standaard worden de te beoordelen VLen getoond.

1. Kies **Beoordelen**, en de VL wordt geopend.
2. Wil je een zaak aanpassen, klik dan op de zaakregel in het overzicht. Kies **Aanpassen**, motiveer de suggestie onder **Opmerkingen** en sla op met knop **Aanpassen** Kies uitzonderen, en vervolgens **Aanpassen**. De suggestie zie je terug in het overzicht met een aangepast statusicoontje
3. Wanneer je een zaak wilt uitzonderen, klik je op de zaakregel in het overzicht. Kies **Uitzondering**, motiveer de suggestie onder **Opmerkingen** en sla op met knop **Aanpassen**. De suggestie zie je terug in het overzicht met een aangepast statusicoontje.
4. Kies **Accorderen** om de VL met eventuele suggesties op te slaan.

Wanneer er aanpassingen zijn voorgesteld, komt de lijst weer in de werkvoorraad van de record manager. Wanneer de lijst zonder aanpassingen geaccordeerd is, komt deze terecht in de werkvoorraad van de archivaris.

Log nu in als archivaris om de VL te accorderen.

Archivist

Taak: Beoordelen vernietigingslijst (VL) **Doel:** Het controleren van de juistheid van verzamelingen zaken die volgens de record manager vernietigd moeten worden.

Je ziet nu het overzicht van VLen. Je kunt het overzicht aanpassen naar de status (beoordeeld, te beoordelen, alle). Standaard worden de te beoordelen VLen getoond.

1. Kies **Beoordelen**, en de VL wordt geopend.
2. Kies **Accorderen** om de lijst te vernietigen.

Vernietiging van zaken

Nadat de archivaris voor **Accorderen** heeft gekozen, worden op de achtergrond een aantal systeemtaken opgestart. Zo wordt er een bewijs van vernietiging verstuurd en worden de zaken daadwerkelijk vernietigd.

1.3.4 Frequently asked questions

What exactly is deleted by the application?

The application is an interface on top of the [API's voor Zaakgericht Werken](#), as present in for example [Open Zaak](#). If the application has the proper authorizations for the APIs and a destruction list with cases (zaken) is approved, the application will delete:

- The cases in the [Zaken API](#) and all related objects within the same API, including the audit trail.
- All documents (documenten) in the [Documenten API](#), related to the deleted case if the document is not related to any other case. All related objects to the document within the same API are also deleted. If the document is related to another case, only the relation to the deleted case, is deleted.

- All decisions (besluiten) in the [Besluiten API](#), related to the deleted case. All related objects to the decision within the same API are also deleted.

Are things really deleted?

Yes! Deleting or destroying cases (zaken) will remove the record from the database. It's not just a flag that is set on the deleted case.

I accidentally deleted a case, can I get it back?

No! Unless you have a backup of the data, you cannot undo a deletion or get the data back.

Is related data, not part of the API's voor Zaakgericht Werken, deleted?

The application destroys cases and related documents and decisions in the [API's voor Zaakgericht Werken](#). The application has no direct control over data that is stored in other applications, registers, APIs or components.

It's the responsibility of the record manager or archivist to make sure that data, related to the case that is deleted, is also deleted.

There are some technical considerations that can be made to delete related data automatically when the case is deleted.

See: *Integration tips for software suppliers*