

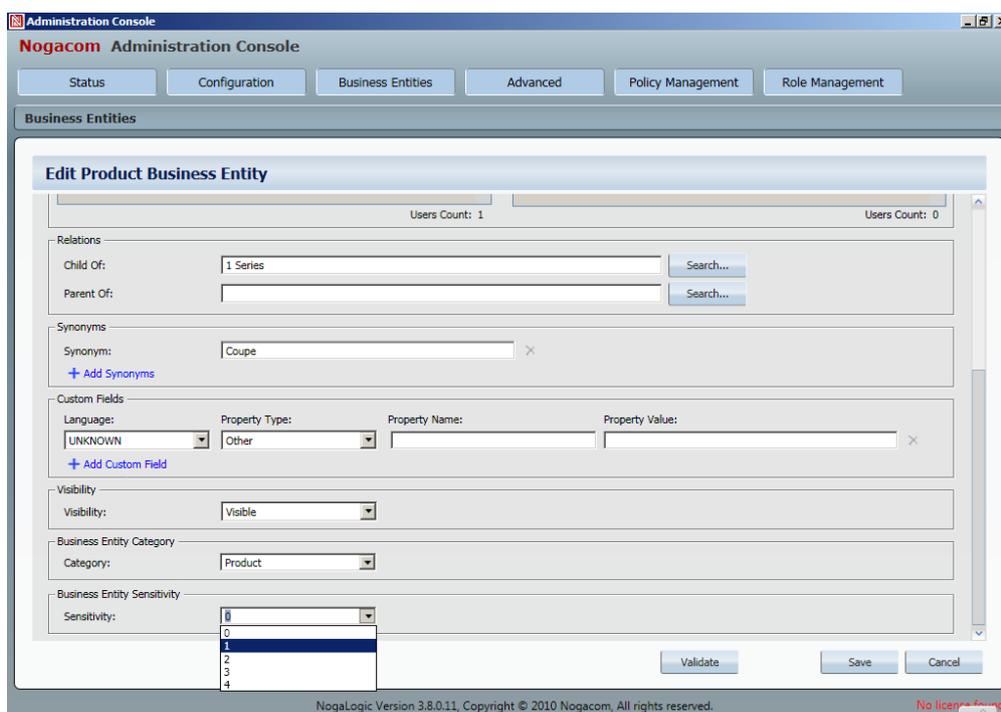
## NogaLogic sensitivity concept

It is a multi – level concept which targets sensitivity through various ways. NogaLogic presents the results in many levels inside the product. The starting point is to answer the question when content becomes sensitive?

1. Document includes sensitive information related to the business (business plan, financial information, customer info etc.)
2. Documents tagged as 'confidential / top secret' etc.
3. When certain 2 or more pieces of business information occur in the same document this makes it sensitive
4. Document contains Personally Identifiable Information (PII)
5. Data is structured in specific templates (e.g invoice, patient record)
6. Document contains specific regular expressions (credit card, patient record)
7. Contains information deemed sensitive by regulations
8. Contains information needed for eDiscovery
9. Contains an electronic business data record
10. Contains certain meta data/properties tags (such as a specific author)
11. External input from 3rd party product (e.g. DLP), predefined lexicons/dictionaries
12. By Management decision

The following description answers the question how to present **Sensitivity** in an Information Management / Governance tool like NogaLogic

### 1. BE sensitivity



The screenshot shows the 'Administration Console' interface for NogaLogic. The main menu includes 'Status', 'Configuration', 'Business Entities', 'Advanced', 'Policy Management', and 'Role Management'. The 'Business Entities' section is active, displaying the 'Edit Product Business Entity' form. The form contains the following fields and sections:

- Users Count:** 1 (left) and 0 (right)
- Relations:** Child Of: 1 Series, Parent Of: (empty)
- Synonyms:** Synonym: Coupe
- Custom Fields:** Language: UNKNOWN, Property Type: Other, Property Name: (empty), Property Value: (empty)
- Visibility:** Visible
- Business Entity Category:** Product
- Business Entity Sensitivity:** 0 (selected)

Buttons at the bottom include 'Validate', 'Save', and 'Cancel'. The footer indicates 'NogaLogic Version 3.8.0.11, Copyright © 2010 Noga.com. All rights reserved.' and 'No license found!'.

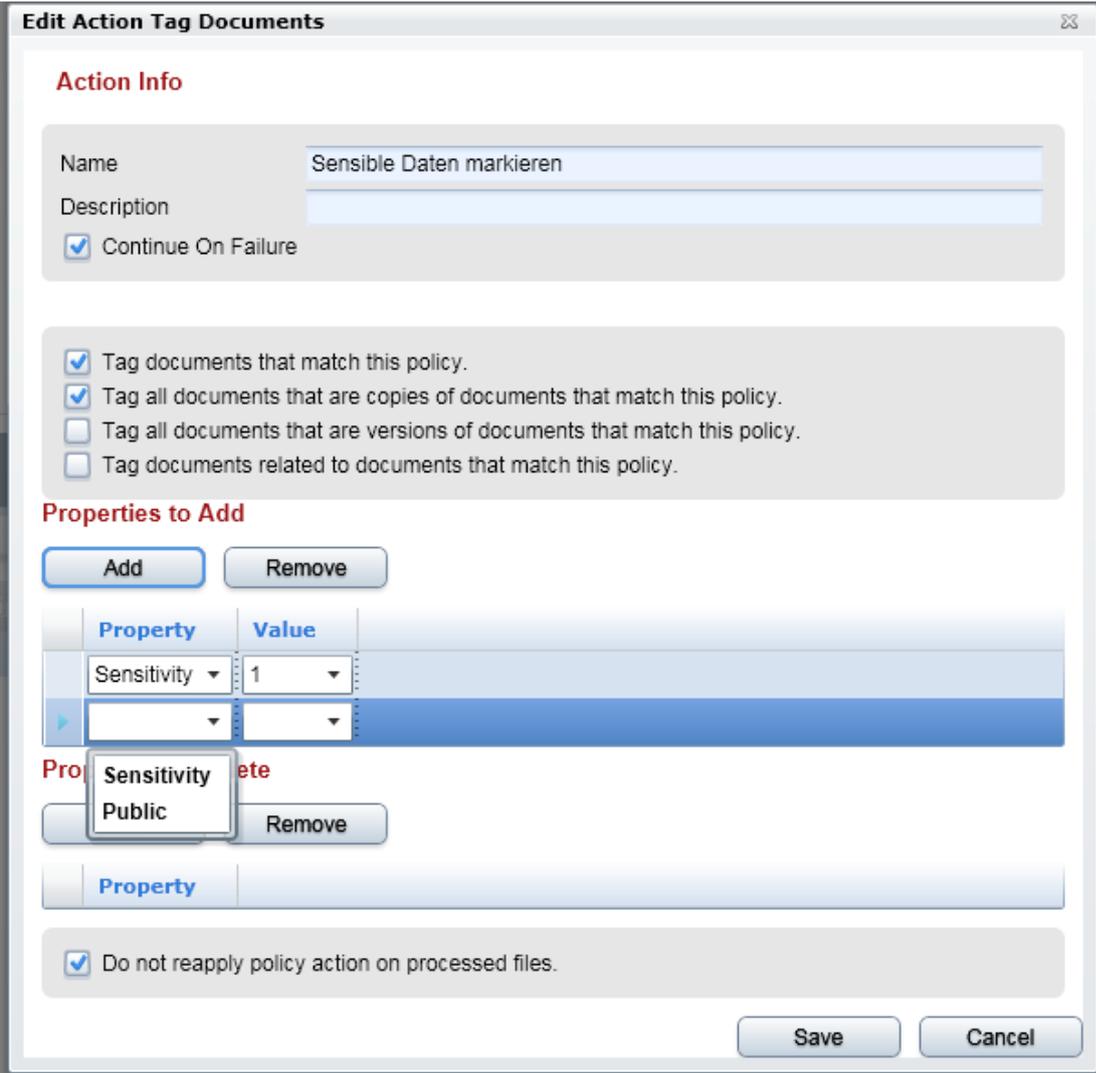
How to handle:

- Pre-define some of the BE's like Public and Sensitive
  - 0 = public
  - 2 = sensitive

Due to this two classes you can separate documents related to this BE's. You can now split the sensitive category in more classes like: Confidential = 1 or secret = 3 or top secret =4

- 0 = public
  - 1 = confidential
  - 2 = sensitive
  - 3 = secret
  - 4 = top secret
  - 5 = for your eyes only
  - Involve Departments in helping to define the department related BE's and its sensitivity
  - Collect them in an Excel Sheet and update later on the BE's
- or
- Extract them from known sources like Active Directory or CRM or Databases or ...

### Select the values from the pre-defined catalogue



**Edit Action Tag Documents**

**Action Info**

Name: Sensible Daten markieren

Description:

Continue On Failure

Tag documents that match this policy.

Tag all documents that are copies of documents that match this policy.

Tag all documents that are versions of documents that match this policy.

Tag documents related to documents that match this policy.

**Properties to Add**

Add Remove

Property	Value
Sensitivity	1

Property: Sensitivity

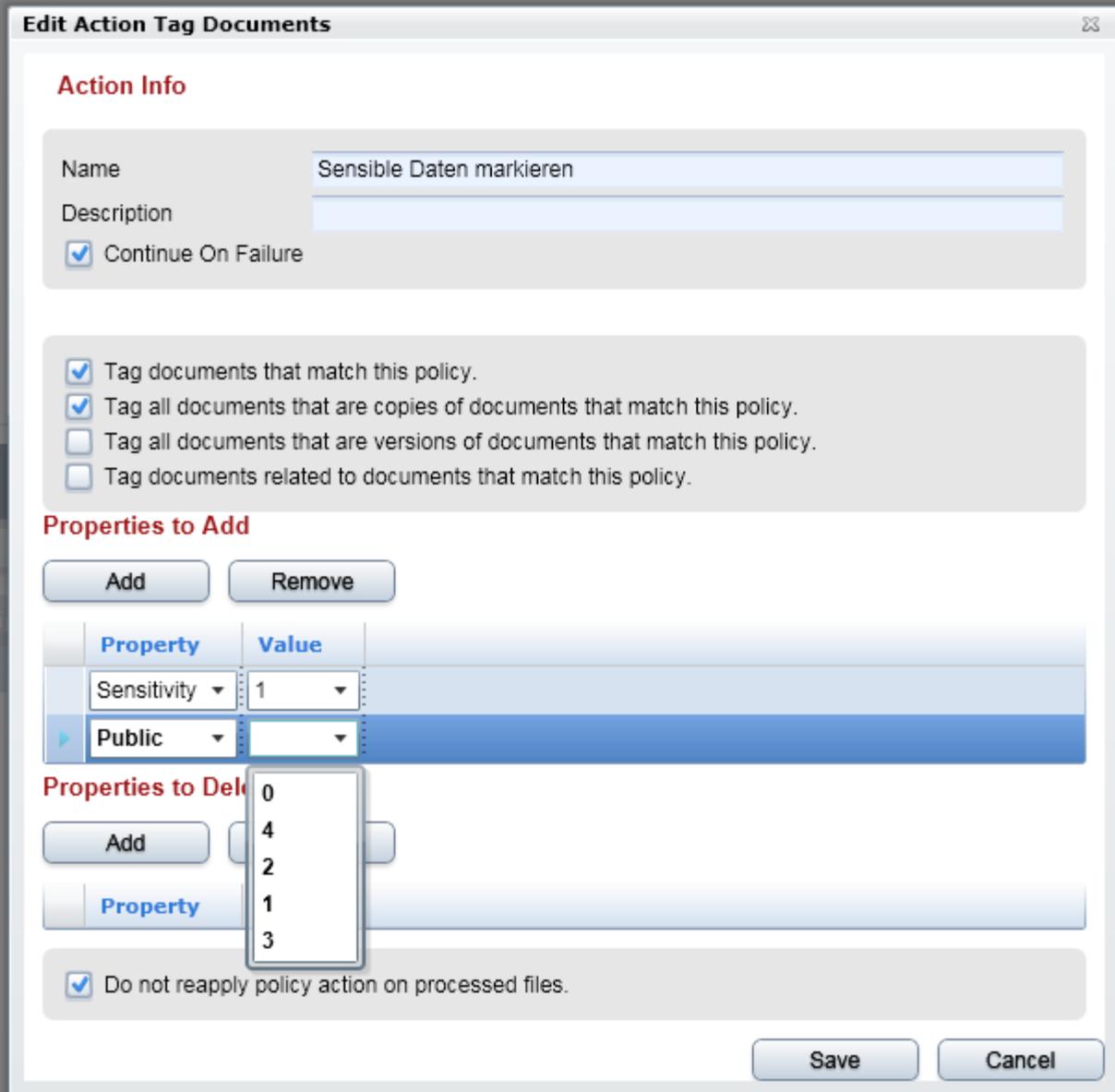
Public Remove

Property

Do not reapply policy action on processed files.

Save Cancel

Update the right value to the right category by selecting the drop down box



**Edit Action Tag Documents**

**Action Info**

Name: Sensible Daten markieren

Description:

Continue On Failure

Tag documents that match this policy.

Tag all documents that are copies of documents that match this policy.

Tag all documents that are versions of documents that match this policy.

Tag documents related to documents that match this policy.

**Properties to Add**

Add Remove

Property	Value
Sensitivity	1
Public	

**Properties to Delete**

Add

Property

Do not reapply policy action on processed files.

Save Cancel

## **Other NogaLogic ways to determine and manage sensitivity cases**

### **2. Sensitivity Views = collecting all sensitive data and save it as a view**

- Each view now can be consolidated until it is precisely showing the result you want to
- Involve Departments in helping to define the views
- Let the views been shown in the Dashboard
- Or add some specific views to the Refinement of the BE tree (see also 8.)

### **3. Tagging through Policy Management**

- Based on the views you can tag the related documents with a value you already pre-defined or you can define on the fly. Recommendation is to pre-define it!
- Use the tagging for 3<sup>rd</sup> party products like DLP

### **4. Sensitivity classes defined as a catalog for Policy Management usage**

- A picture will follow
- Define the Property and the value for selecting it later on in the policy management

### **5. Meta Data has already such information**

- If data already contains such information in its Meta Information (Properties) we can use it and manage data accordingly

### **6. System API: Gets input from 3<sup>rd</sup> party system**

- Get an import through our System API and use it accordingly

### **7. Dash Board is showing sensitivity views**

### **8. Fast access: Pre-defined sensitive views are shown in the BE tree**