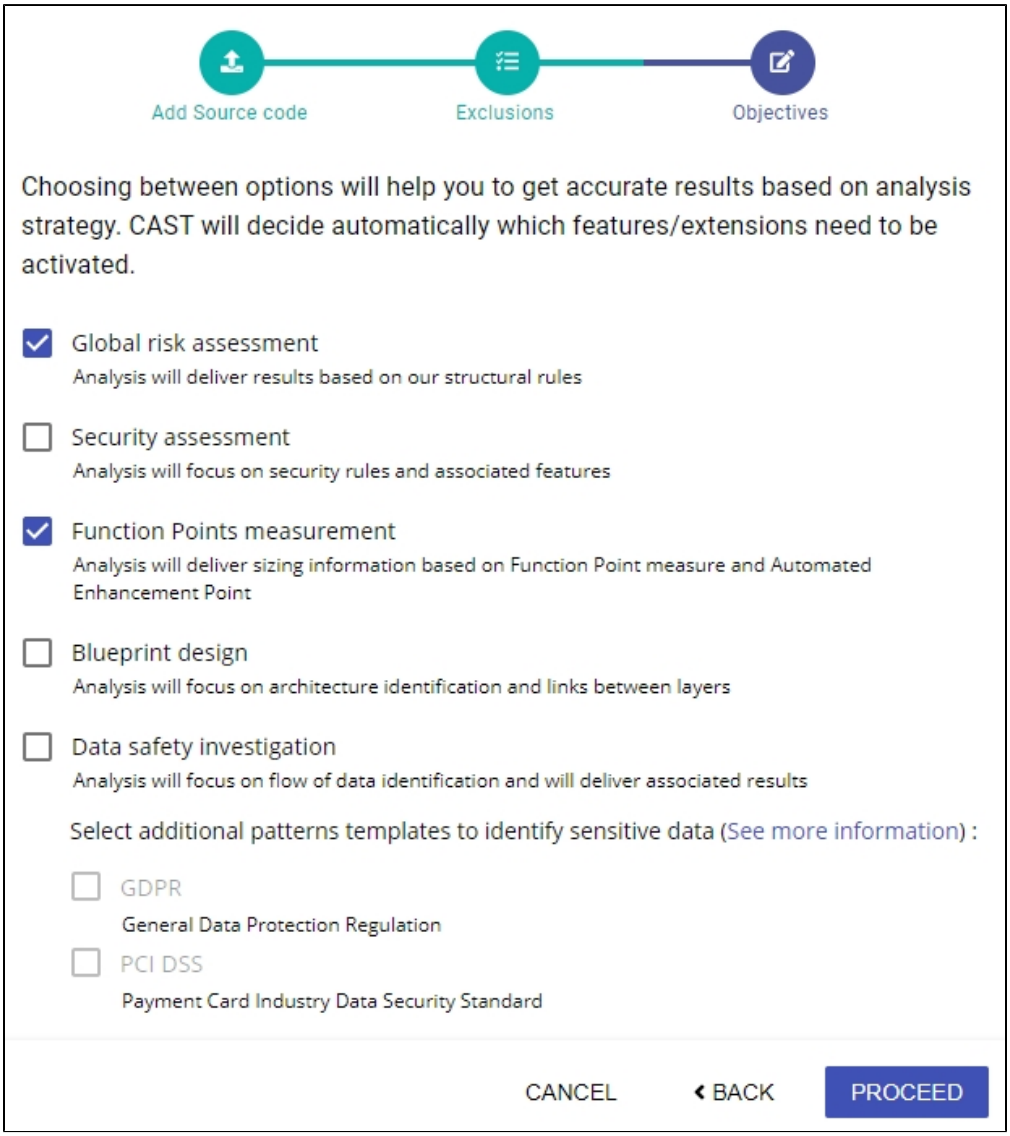
Choose objectives step 3

Choose Objectives

Objectives is an optional feature that is designed to **pre-configure an analysis** (install specific extensions, set specific settings etc.) based on the results you require:



When you have made your option choices (see **below**), click **PROCEED:**

- if the **Run Analysis** option is **disabled**, the **version will be added** and will appear in the **Application - Versions** screen.
- if the **Run Analysis** AND **Take a snapshot** options are **enabled**, the **analysis/snapshot** will be **actioned immediately**.

- When enabling any of the **Objectives**, it is recommended to allow **Alpha and Beta extensions** to be installed via the **Extension Strategy option**, because some of the extensions that are installed automatically via the Objectives feature are currently only in Alpha /Beta release. If Alpha/Beta extensions are not permitted to be installed, the results of the selected objectives will not be produced.
- When an extension whitelist is in use via the **Extension Strategy option**, any extensions that are automatically installed by a selected Objective and which are not present in the white list will cause the analysis **to stop**.
- If you do not wish to use any of the objectives offered, **untick all options**. This will ensure that no additional extensions (over and above what you have defined and what has been automatically discovered) will be installed and no additional options will be enabled automatically.
- If you are adding a version N+1 (i.e. you have already created a version and generated a snapshot and are now working on the next version) and you tick the option **Same as previous configuration** in Step 1, the same objectives will be applied as in the previous version.
- If you have generated a snapshot and enabled various objectives, and you then edit the version and generate a new snapshot, the same objectives will be applied.

Options available

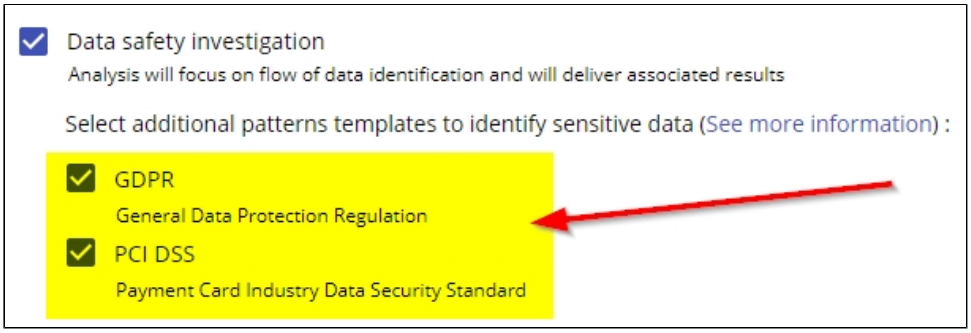
Option	Default settings	Description
Global risk assessment	Active	This option focuses on **risk assessments** by adding additional structural rules to the analysis. Selecting this option will cu the following **extensions** (in addition to any that are **discovered,** set to **force install** or those that are **automatically acti extensions**): • **com.castsoftware.qualitystandards** • **com.castsoftware.jeerules** • **com.castsoftware.dotnetweb** • **com.castsoftware.systemlevelrules** • **com.castsoftware.automaticlinksvalidator**

Security assessment	Inactive	This option focuses on **user input security assessments** for **JEE/NET technologies**. Selecting this option will currently:
		• install the following **extensions** (in addition to any that are **discovered,** set to **force install** or those that are **automa shipped extensions**):
		  • **com.castsoftware.qualitystandards**
		  • **com.castsoftware.automaticlinksvalidator**
		  • **com.castsoftware.securityforjava** (JEE only)
		  • **com.castsoftware.jeerules** (JEE only)
		  • **com.castsoftware.dotnetweb** (.NET only)
		• enable the following **options**:
		  • **Application - Security Dataflow** for the discovered technologies (JEE and/or .NET)

Functional points measurement	Active	This option focuses on **function points measurement**. Selecting this option will currently install the following **extensions** any that are **discovered,** set to **force install** or those that are **automatically active / shipped extensions**): • **com.castsoftware.automaticlinksvalidator** If you are using a CAST global license that **does not include EFP**, then this option will not produce any results.
Blueprint design	Inactive	This option focuses on **architecture identification and links between layers**. Selecting this option will currently install th **nsions** (in addition to any that are **discovered,** set to **force install** or those that are **automatically active / shipped exte** • **com.castsoftware.automaticlinksvalidator**
Data safety investigation	Inactive	This option focuses on **flow of data identification and will deliver associated results**. Selecting this option will currentl following **extensions** (in addition to any that are **discovered,** set to **force install** or those that are **automatically active / extensions**): • **com.castsoftware.automaticlinksvalidator** • **com.castsoftware.datacolumnaccess** • **com.castsoftware.mainframe.sensitivedata** (in **AIP Console 1.26**) **GDPR / PCI DSS**

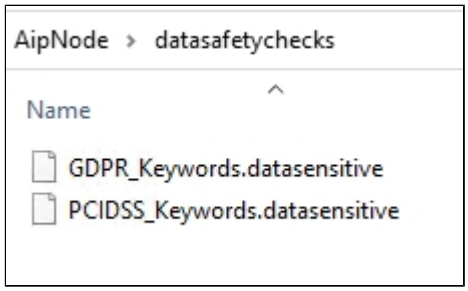
- These options are ONLY currently taken into account for **Mainframe technolgies** (analyzed via the **com.cas mainframe** and **SQL technologies** (analyzed via the **com.castsoftware.sqlanalyzer** extension).
- These options do not provide a certification for GDPR and PCI DSS. Their aim is to help identify sensitive da particular contexts.
- It is still possible to provide your own patterns (see **Mainframe Sensitive Data** and **Data Column Access**).

Two additional options are available (in **AIP Console 1.26**) specifically enabling a check of a set of predefined sensitive **k** d to **GDPR** (General Data Protection Regulation) and/or **PCI-DSS** (Payment Card Industry Data Security Standards) data:



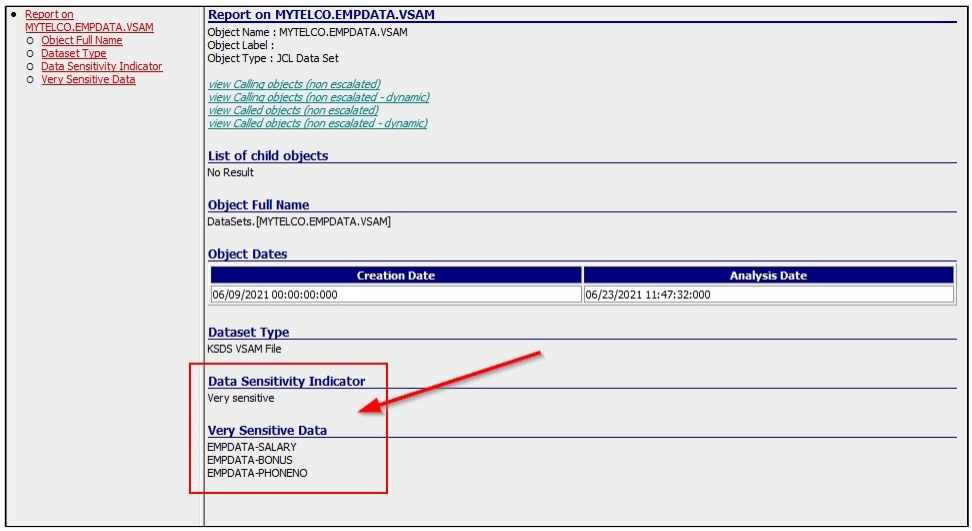
Each option corresponds to one **.datasensitive** file located in the following location on the AIP Node:

```
%PROGRAMDATA%/CAST/AipConsole/AipNode/datasafetychecks
```



In other words, enabling the **GDPR** option (for example) will force the check using the keywords defined in **GDPR_Keywo datasensitive**. When the analysis runs, the predefined .datasensitive file corresponding to the chosen option is sent to the ISA/{appGuid}/DataSafety) and any key words defined in them will be checked. If any key words are found in the source c be added in the analysis results on the object in question. This can be seen as below:

Click to enlarge



Click to enlarge

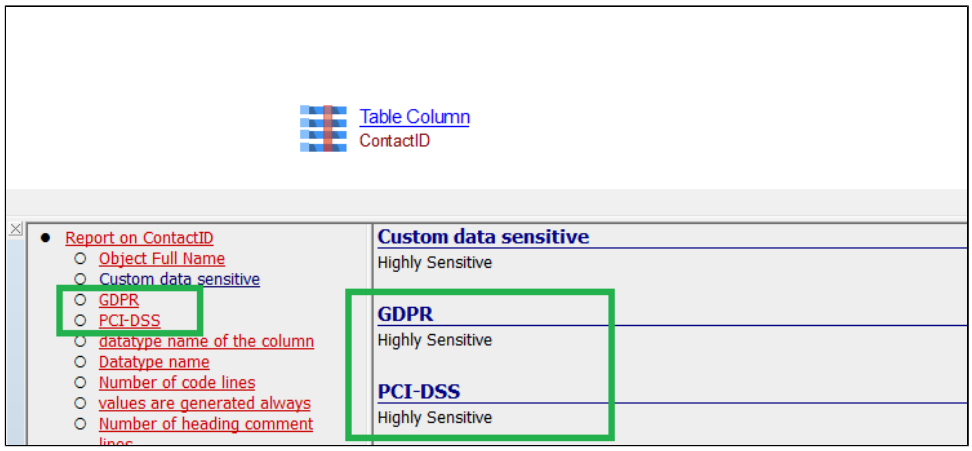


Table Column
ContactID
Report on ContactID
Object Full Name
Custom data sensitive
GDPR
PCI-DSS
datatype name of the column
Datatype name
Number of code lines
values are generated always
Number of heading comment
Custom data sensitive
Highly Sensitive
GDPR
Highly Sensitive
PCI-DSS
Highly Sensitive