4.1.6. Breaches package.
Figure 12 shows the `Breaches` package. `Breaches` are unplanned situations (*e.g.*, attacks, bugs) that hinder personal data security. When a breach occurs, GDPR prescribes `Breaches` management rules that revolve around a `Breaches` register.

`Breaches` must all be documented in detail. Their `nature`, their occurrence date (`createdAt` attribute of `Breach` class), their impact (`Consequence` class) and the `Measures` taken to remedy them are required to be logged.

In order to precisely define what piece of personal data is impacted, `Breaches` must also be linked to `Data` and `DataSubjects`. The number of affected `DataSubjects` is important to know too; it can be calculated.

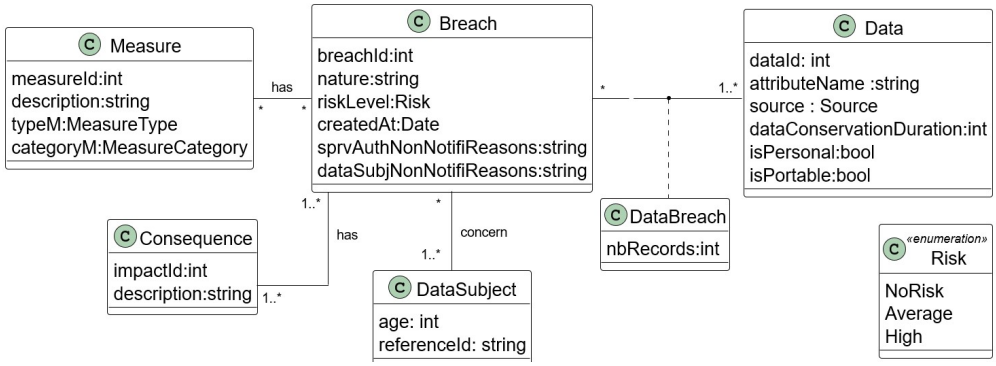

Figure 12: Breaches package.

When a `Breach` of `High` risk level is detected, the supervisory authority and the affected `DataSubjects` have to be informed. If the risk level is moderate (`Average` risk value) it is not mandatory to inform the supervisory authority and the affected `DataSubjects`. In that case, a justification for the lack of notification must be given (respectively using the `sprvAuthNonNotifReasons` and `dataSubjNonNotifReasons` attributes of the `Breach` class).

4.1.7. Documents package.
Figure 13 depicts the classes of the `Documents` package which gathers the various legal documents used in privacy management. There are four types of legal documents, relative to either `Processings`, `Consents` or `Breaches`:

- **Records of processing activities** (`RecordsProcessingActivities` class). Application owners must maintain a `RecordsProcessingActivities` as described in GDRP, Art. 30. The prescribed informations are available from the `Actors`, `Data` and `Processings` packages and automatically fed into this document.
- **Contracts** (`Contract` class). As explained previously (*see* `Consents` package), the `Contract` document of a `DataSubject`, lists all the `Processings` they consented to. It

specifies how personal data will be processed and what the purposes of `Processings` are.

- **Records of breaches** (`RecordBreaches` class). As explained previously (in the Breaches package), the `RecordBreaches` is key to both log data `Breaches` and notify the supervisory authority and affected `DataSubjects`. It contains detailed information on data breaches, including their nature or consequences.
- **Data Protection Impact Assessment (DPIA) report** (`DPIAReport` class). DPIA is a process to assess risks to individuals' privacy before conducting high-risk data processing activities (GDPR, Art. 35). A `DPIAReport` identifies potential risks and mitigation measures.

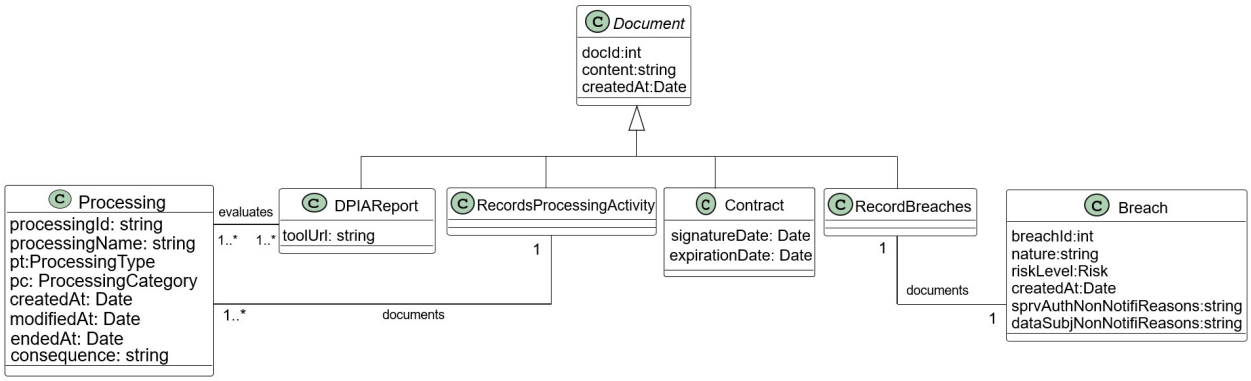

Figure 13: Documents package.

Records for processings activities, records for breaches, and contracts are automatically generated from the information available in instantiated classes of their respective related package. DPIA is applicable to specific processings (*e.g.*, that manipulate health-related data). This work, does not cover DPIA because it would necessitate to catalog all these specific cases and their associated data (*e.g.*, risks and their impact) for which dedicated tools already exist. The interested reader can refer to PIA tool [14], which offers a dedicated software tool and complementary documentation to assist this task. The URL of the tool is available for reference in the `toolUrl` attribute of the `DPIA` class.