Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR

Damiano Torre 1 · Mauricio Alferez 1 · Ghanem Soltana 1 · Mehrdad Sabetzadeh 2 1 · Lionel Briand 1 2

Received: date / Accepted: date

Damiano Torre
E-mail: damiano.torre@uni.lu
Mauricio Alferez
E-mail: mauricio.alferez@uni.lu
Ghanem Soltana
E-mail: ghanem.soltana@uni.lu
Mehrdad Sabetzadeh
E-mail: m.sabetzadeh@uottawa.ca
Lionel Briand
E-mail: lionel.briand@uni.lu

1 SnT Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
2 School of Electrical Engineering and Computer Science, University of Ottawa, Canada
Appendix A

In this Appendix, we present (a) the packages of the CM presented in Fig. 1 and the traceability of the packages to the GDPR in Section 1, (b) the glossary (Section 2), (c) the compliance rules in plain English (Section 3), and (d) the set of variation points (Section 4).

1 Packages traceability to the GDPR

Principles package is showed in Fig. 2 and its traceability to the GDPR is described in Table 1.

| Class                | Traceability to GDPR |
|----------------------|-----------------------|
| Accuracy             | Article 5             |
| Data Minimization    | Article 5             |
| Demonstration        | Articles 5, and 25    |
| Fairness and         | Article 5             |
| Transparency         |                       |
| Integrity and        | Article 5             |
| Confidentiality      |                       |
| Lawfulness           | Article 5             |
| Lawfulness Evidence  | Article 5             |
| Lawfulness Source    | Article 6             |
| Obligation Source    | Article 6             |
| Principle            | Abstract concept      |
| Purpose Limitation   | Article 5             |
| Storage Limitation   | Article 5             |

Data Processing package is showed in Fig. 3 and its traceability to the GDPR is described in Table 2.

| Class                   | Traceability to GDPR |
|-------------------------|-----------------------|
| Consent                 | Articles 4, 7, and 8  |
| Data Processing         | Article 4             |
| Filing System           | Articles 2, and 4     |
| Personal Data           | Articles 4, 9, and 10 |
| Purpose                 | Articles 5, and 13 to 15 |

Data Subjects package is showed in Fig. 4 and its traceability to the GDPR is described in Table 3.

| Class                      | Traceability to GDPR |
|----------------------------|-----------------------|
| Child Data Subject         | Article 8             |
| Data Subject               | Article 4             |
| Natural Person             | Abstract concept      |
| Responsible Parent         | Article 8             |

Main Actors package is showed in Fig. 6 and its traceability to the GDPR is described in Table 4.

| Class                         | Traceability to GDPR |
|-------------------------------|-----------------------|
| Accreditaion Body             | Article 43            |
| Processing Activity Record    | No mapping the law    |
| Actor                         | Abstract concept      |
| Certification Body            | Article 43            |
| Communication                 | Articles 31, 57, 58, and 33 |
| Contract Agreement            | Article 28            |
| Controller                    | Abstract concept      |
| Country                       | Article 3             |
| Court                         | Articles 78, 79, and 81 |
| Data Processor                | Articles 4, 28, and 29 |
| Data Protection Officer       | Articles 37 to 39     |
| EU Data Protection Officer    | Articles 68 to 76     |
| Group Of Undertakings         | Articles 4, and 47    |
| Joint Controllers             | Articles 4, and 26    |
| Legal Authority               | Abstract concept      |
| Main Intervenant              | Abstract concept      |
| Obligation                    | Articles 24 to 31     |
| Processor                     | Abstract concept      |
| Recipient                     | Chapter 5             |
| Representative                | Articles 4, 27, and 80 |
| Supervisory Authority         | Articles 4, and 51 to 59 |
| Third Party                   | Articles 4, and 44    |
| Undertaking                   | Articles 4, and 47    |
| Data Controller               | Articles 4, and 24    |
Fig. 1 Package Representation of the CM

**Data Subject Rights package** is showed in Fig. 7 and its traceability to the GDPR is described in Table 5.

| Class                      | Traceability to GDPR |
|----------------------------|----------------------|
| Notification               | Article 19           |
| Right                      | Abstract concept     |
| Right To Portability       | Article 20           |
| Right To Access            | Article 15           |
| Right To Be Informed       | Articles 13 to 14    |
| Right To Erasure           | Article 17           |
| Right To Not Be Part Of A Decision | Article 22         |
| Right To Object            | Article 21           |
| Right To Restriction       | Article 18           |
| Right To Rectification     | Article 16           |
| Information                | Articles 13 to 15    |
Compliance package is showed in Fig. 8 and its traceability to the GDPR is described in Table 6.

### Table 6 Compliance Package

| Class                        | Traceability to GDPR                  |
|------------------------------|---------------------------------------|
| Breach                       | Articles 4, 33, and 34                 |
| Certification                | Article 42                             |
| Code Of Conduct              | Article 40                             |
| Conduct Rule                 | Article 40                             |
| Consultation                 | Article 36                             |
| Data Protection Impact Assessment | Article 35                         |
| DPIA Information             | Article 35                             |
| DPIA Motivation              | Article 35                             |
| Organizational               | Articles 24, 28, and 32                |
| Record Activity              | Article 30                             |
| Risk                         | Article 32                             |
| Security Measure             | Abstract concept                      |
| Technical                    | Articles 24, 28, and 32                |
| View                         | Article 35                             |

Data Transfer package is showed in Fig. 9 and its traceability to the GDPR is described in Table 7.

### Table 7 Data Transfer Package

| Class                        | Traceability to GDPR                  |
|------------------------------|---------------------------------------|
| Adequacy Decision            | Article 45                             |
| Adequacy Evidence            | Article 45                             |
| Administrative Arrangement   | Article 46                             |
| Authorization                | Article 46                             |
| Binding Corporate Rules      | Article 47                             |
| Clause                       | Articles 46 to 47                      |
| Commitment                   | Articles 46, and 49                    |
| Contact Based                | Abstract concept                      |
| Contact Information          | Articles 46 to 47                      |
| Cross Boarder Processing     | Abstract concept                      |
| Data Transfer                | Article 44                             |
| International Binding        | Article 49                             |
| Legal Basis                  | Abstract concept                      |
| Local Processing             | No mapping to the law                 |
| Standard Contractual Clauses | Article 46                             |
| Transfer Derogation           | Article 49                             |
| In house Processing          | WP 244, and Article 29                 |

Administration package is showed in Fig. 5 and its traceability to the GDPR is described in Table 8.

### Table 8 Administration Package

| Class                        | Traceability to GDPR                  |
|------------------------------|---------------------------------------|
| Dispute                      | Articles 78, 79, and 81                |
| Complaint                    | Articles 4, and 77                    |
| Communication_Trace          | Article 77                             |
| Report                       | Article 59                             |
| Corrective_Action            | Article 58                             |
| Infringement                 | Article 83                             |
| Investigation_Task           | Article 57                             |

Enumeration package. We describe in detail the Enumeration package showed in Fig. 10.
Fig. 2 Principles Package

Fig. 3 Data Processing package
Fig. 4 Data Subjects Package

Fig. 5 Administration Package
Fig. 9 Data Transfer Package
2 Glossary

As follows, we present the glossary related to the CM’s packages previously presented.

**Country Code class:** Lists the abbreviation codes for countries. The ISO Country Codes standard where used for the literals, e.g., LU denotes Luxembourg.

**Actor Type class:** Lists the possible types for a real actor involved in the data processing.

| Literal          | Description                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Natural Person   | A natural person is a person that is an individual human being.                                                                               |
| Legal Person     | A legal person is any individual, company, or other entity which has legal rights and is subject to privileges and obligation such as having the ability to enter into contracts, to sue, and to be sued. |
| Non Profit Organization | When they are formed to further cultural, educational, religious, professional, or public service objectives. Their start-up funding is provided by their members, trustees, or others who do not expect repayment, and who do not share in the organization’s profits or losses which are retained or absorbed. |
| Official         | Any establishment recognized as an Authority entity or a public body.                                                                          |
| Public Organization | When they are owned and operated by the government and exist to provide services for citizens. Often, organizations in the public sector do not seek to generate a profit. |
| Enterprise       | It is a business or a company.                                                                                                              |
| International Organization | An international organization is an organization with an international membership, scope, or presence.                                             |
| Information Society Service | An information society service is any society/person that provides service provided, via electronic means upon an individual request from a user. |

**Restriction Right Reason class:** Lists the situations where data processing can be restricted.

| Literal          | Description                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Contested Accuracy | If the data subject (DS) contest the accuracy of the data concerning him or her.                                                              |
| DS Objects       | If the DS has lodged a complaint against the processing.                                                                                      |
| Unlawful Processing | If the processing has no legal basis.                                                                                                         |
| Data no Necessary | If the personal data of a data subject is no longer needed for a given processing.                                                             |
| Other            | Groups the other exceptional situations where the processing can be restricted.                                                               |
**Processing Context class**: Provides standard general contexts for which personal data is processed.

| Literal                      | Description                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Employment                   | A relationship between two parties, usually based on a contract where work is paid for, where one party is the employer and the other is the employee.                                                           |
| Vital Interests              | It is necessary to protect life and death of individuals.                                                                                                                                                   |
| Membership Organization      | Any organization that allows people to subscribe, and often requires them to pay a membership fee or subscription.                                                                                             |
| Legal and Criminal Investigation | The study of facts, used to identify and prove the guilt of an accused person according to the law.                                                                                                           |
| Public Interest              | Any processing conducted in the interest is "the welfare or well-being of the general public".                                                                                                             |
| Preventive Medicine          | It consists of measures taken for disease prevention, as opposed to disease treatment.                                                                                                                     |
| Public Health                | The science of protecting the safety and improving the health of communities through education, policy making and research for disease and injury prevention.                                                   |
| Research                     | The systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.                                                                                 |
| Statistical Purposes         | Any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results.                                                                |
| EU Foreign and Security Policy | EU foreign and security policy, which has developed gradually over many years, enables the EU to speak and act as one in world affairs.                                                                        |
| Persona or Household Activity | Activities which are exclusively personal or household.                                                                                                                                                     |
| Prevention Threats to Public Security | The activity of identification of possible threats in order to prevent threats for the public security.                                                                                                  |
| Offering Goods or Services   | The process (carried out by an actor) of offering goods or services.                                                                                                                                       |
| EU Behaviour Monitoring or Profiling | The process of monitoring or profiling the behaviour of individuals that reside within the EU.                                                                                                               |
| Behaviour Monitoring or Profiling | The process of monitoring or profiling the behaviour of data subject.                                                                                                                                       |
| EU Security Activity         | The EU activities aimed at keeping secure the EU.                                                                                                                                                           |
| OTHER                        | Any additional processing context not in the enumeration.                                                                                                                                                   |
Data Category class: Lists the different categories of personal data envisaged by GDPR.

| Literal           | Description                                                                 |
|------------------|-----------------------------------------------------------------------------|
| Racial or Ethnic | Any data that might reveal the race or ethnicity of an individual.           |
| Religious or Philos. Believes | Any data that might reveal the religious or philosophical believes of an individual. |
| Political Opinion | Any data that might reveal the political opinions of an individual.         |
| Health           | Any data that reveals information about the health status of a given person. |
| Sex Life         | Any data that reveals information about the sexual orientations and life a given person. |
| Genetic          | Data relating to the inherited or acquired genetic characteristics of a natural person. |
| Biometric        | Physical, physiological or behavioural characteristics of a natural person. |
| Judicial         | Data relating to criminal convictions and offenses                          |
| Other Personal Data | Other types of personal data that might make the DS identifiable.         |

Operation Type class: Provides some standard types of automated data processing.

| Literal | Description                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Collecting | The activity of bringing or gather together personal data.                                                                                                                                                 |
| Profiling | The activity of recording and analysis of a person’s psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people. |
| Archiving | The activity of transferring (personal data) to a less frequently consulted storage.                                                                                                                                 |
| Recording | The action or process of recording personal data for subsequent use.                                                                                                                                                                                                 |
| Organizing | The activity of arranging/ordering personal data systematically.                                                                                                                                                                                                       |
| Structuring | The activity constructing or arranging personal data according to a give a pattern.                                                                                                                                                                                    |
| Storing | The activity of keeping or accumulating personal data for future use.                                                                                                                                                                                                 |
| Altering | The activity of changing in character or composition the personal data, typically in a comparatively small but significant way.                                                                                                                                       |
| Retrieving | The activity of getting or bringing personal data back from somewhere.                                                                                                                                                                                               |
| Consulting | The activity of accessing personal data.                                                                                                                                                                                                                           |
| Using | The activity of taking, holding, or deploying personal data as a means of processing the data.                                                                                                                                                                         |
| Transmitting | The activity of passing personal data on from one person, organization, etc. to another.                                                                                                                                                                              |
| Restricting | The activity of limiting personal data somehow.                                                                                                                                                                                                                      |
| Erasing     | The activity of delegating recorded personal data.                                                                                                                                                                                                                   |
| Destroying | The activity of completely eliminating personal data from more than one support and from one or more tiers.                                                                                                                                                           |
| Other      | Additional specific processing types can be specified.                                                                                                                                                                                                                 |
**Technical Measure Type class:** Provides some standard types for technical measure that can be implemented as safeguards to protect personal data and comply with GDPR.

| Literal  | Description                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Access Control | Policy to limit access to personal data for an authorized employee to ensure that employees have access only to information or systems applicable to their job. |
| Data Protection | It is the branch of information security dealing with the proper handling of data concerning consent, notice, sensitivity, and regulatory concerns. It specifies the relationship between the collection and dissemination of data, technology, and the legal and political issues surrounding them. |
| Authentication | The process or action of proving or showing some credential to be valid.                                                                    |
| Pseudonymization | The activity of processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. |
| Encryption | Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access. |
| Transmission Control | It is responsible for the transmission of personal data.                                                                                   |
| Password Polices | A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. |
| Backups Recovery | Backups refer to make a copy of the data which should be replicated to another device or location. That data may be used to restore the original after a data loss event. |
| Run the checking | It is an analysis and execution approach based on extracting information from a running system and using it to detect and possibly react to observed behaviours satisfying or violating certain properties such as unauthorized access. |
| Other | Other data protection technical measure can be specified.                                                                                  |

**Organizational Measure Type class:** Provides some standard types for organizational measures that can be implemented as safeguards to protect personal data and comply with GDPR.

| Literal  | Description                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Audit | Inspection of an organization and system functioning, often by an independent body.                                                         |
| Staff Training | Training employees and raising awareness about GDPR and best practices to protect personal data.                                             |
| Dedicated Personal Protection Policy | Dedicate some employee to the specific task of ensuring and monitoring compliance with GDPR. Protection policy is a document which provides guidelines to users on the processing, storage, and transmission of sensitive information. |
| Study State of Art | Be up-to-date and informed about the latest technology and organizational advances in terms of data protection.                                      |
| Study Competition | Study and analyze the technical and organizational measures applied by similar companies (competition) to protect personal data.                   |
| Other | Other protection organizational measures can be specified.                                                                                  |
Denial Erasure Reason class: Specify the situation where, without further authorizations, a controller can deny or request for data erasure made by a given DS.

Table 16 Denial Erasure Reason class

| Literal                      | Description                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Freedom Expression Information | If the controller deems that the processing is done in under the freedom of expression (and does not violate other rights).                  |
| Compliance Legal Obligation   | If the controller must keep the data to comply to legal obligation.                                                                           |
| Public Interest               | If the controller must keep the data to for public interest related reasons.                                                                   |
| Archiving Purposes            | If the controller must keep the data for archive purposes.                                                                                   |
| Defense Legal Claims          | If the controller must keep the data for the defense of legal claims (data is kind of a legal proof).                                               |

Lawfulness Sources class: Lists the possible legal basis, as envisaged by the GDPR, for a given processing of personal data.

Table 17 Lawfulness Sources class

| Literal                      | Description                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| By Consent                   | The processing is enabled by a consent. Consent means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| Performance of Contract      | The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. |
| Legal Obligation             | It covers processing that is necessary to fulfill a legal obligation to which the data controller is subject. Examples include obligations in the fields of employment and social security, including those that require processing sensitive (now known as "special category") personal data. |
| Protect Vital Interests      | The processing is necessary to protect the vital interests of the DS. This is relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing. |
| Public Interest              | The processing is necessary for Public interest reasons. Examples include taxation, reporting crimes, humanitarian purposes, preventive or occupational medicine, public health, social care, quality and safety of products, devices and services, and election campaigns. |
| Legitimate Interest          | A legitimate interest is a clearly articulated benefit to a single company, or to society as a whole, that can be derived from processing personal data in a lawful way. |
| None                         | None of the standard legal basis is possible. This can happen when the processing is not the main reason for which the data was initially collected or when the legal basis for processing is based on a derogation as stated in Article 6. |
**Information Type class:** Summarizes the type of information that controller might provide when exercising the information and access rights for a given individual.

| Literal | Description |
|---------|-------------|
| Contact Details | An individual’s private or personal information by which another person, business, or entity can use to reach the individual. |
| DPO Details | The Data Protection Officer (DPO) information by which another person, business, or entity can use to reach that DPO. |
| Purpose and Lawfulness | The reason for which some personal data are somehow processed according to the law. |
| Data Categories | The different categories of personal data that are involved in the data processing. |
| Recipients | The natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. |
| Transfer Third Countries | Explicitly states whether the processing involves data transfers to third countries. |
| Storage Duration | The storage duration. |
| DS Right | Summarizes the enables DS rights for a given processing. |
| Consent Withdrawal | States whether the consent is withdrawable at any time. |
| Right to Lodge Complaint | Recalls DS that they have the right to lodge a complaint. |
| Data Source | The sources used to gather personal data. |
| Statutory Contractual Requirement | The regulatory obligations that are required by a statutory contractual requirement. (if applicable) |
| Automated Decision | The involved automated decisions that might be linked to the underlying processing. |
| Further Processing | States whether additional (to what already exists) processing of personal data are planned or possible. |
| Right to Receive Copy | Recall DS about their right to receive the personal data concerning him or her in a structured, commonly used and machine-readable format. |
**DPIA Information Type class**: Summarizes the standard type of information that a Data Processing Impact Assessment might contain.

| Literal                  | Description                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Necessity Assessment     | A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.                                    |
| Proportionality Assessment| An assessment of the necessity and proportionality of the processing operations in relation to the purposes.                                                                                                 |
| Measures Description     | The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. |
| GDPR Principle Assessment| An assessment that checks that the processing respects all applicable GDPR principles.                                                                                                                       |
| DS Rights Assessment     | An assessment that checks that the processing respects all applicable DS rights.                                                                                                                             |
| Freedoms Assessment      | An assessment of the risks to the rights and freedoms of data subjects and others.                                                                                                                           |
| Obligation Assessment    | An assessment that verifies that the involved controllers and processors have fulfilled all their GDPR imposed obligations.                                                                                  |
| Risk Assessment          | Summary of the potential risks related to the processing and how they were mitigated.                                                                                                                        |
| Other                    | Any additional assessment that supports DPIA.                                                                                                                                                               |
**Exception Special Data Category class:** Lists the different possible scenarios where processing of special data categories can be lawful.

| Literal                          | Description                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Consent Permitted by EU         | The special data can be processed when the processing is clearly permitted by the EU law.                                                       |
| Legal Obligation                | The special data can be processed when the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and protection law. |
| Protect Vital Interests         | The special data can be processed when it is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. |
| Legitimate Activities           | The special data can be processed when in the context of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects. |
| Made Public by Subject          | The special data can be processed when the data are manifestly made public by the data subject.                                               |
| Establishment Exercise or Defense Legal Claims | The special data can be processed for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity. |
| Public Service                  | The special data can be processed when the processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which shall be proportionate to the aim pursued. |
| Preventive or Occupational Medicine | The special data can be processed when the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. |
| Health Care                     | The special data can be processed when the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. |
| Historical Research or Statistical | The special data categories can be processed when the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. |
| None                            | No valid reason for processing sensitive data found (non-compliant state).                                                                   |

**Erasure right reason class:** Summarizes the situations where a DS can request the erasures of his or her personal data.

**Risk Severity class:** Defines the level of risk severity related to a given data breach.

| Literal      | Description                                   |
|--------------|-----------------------------------------------|
| Low          | The risk is low.                              |
| Medium       | The risk is deemed to be average.             |
| High         | The risk is deemed to be extremely high.      |
Table 21 Erasure right reason class

| Literal               | Description                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Data no Longer Necessary | It refers to the situation when some specific personal data of a data subject is no longer needed for a given processing.                  |
| Consent Withdrawal    | Once the consent is withdrawn, DS might ask for the erasures of the data concerning him or her.                                             |
| DS Objects            | In case DS objects the processing, DS might ask for the erasures of the data concerning him or her.                                         |
| Unlawful Processing   | DS might ask for the erasures of the data concerning him or her if she deems that the processing personal has no legal basis.              |
| Legal Obligation      | DS might ask for the erasures of the data concerning him or her in order to meet some legal or judicial obligation.                      |

Table 23 DPIA Motivation class: Lists the standard situations where a Data Privacy Impact Assessment (DPIA) is required or recommended.

| Literal                  | Description                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Profiling                | If the processing involves behavior profiling.                                                                                               |
| Significant Legal Impact | A data protection impact assessment shall, in particular, be required in case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. |
| Involves Special or Criminal Data | A data protection impact assessment shall, in particular, be required in case of personal data relating to criminal convictions and offenses. |
| Systematic Monitoring    | A data protection impact assessment shall, in particular, be required in case of systematic monitoring of a publicly accessible area on a large scale. |
| Involves Database Merge  | A DPIA is welcomed when the data processing involves database merging.                                                                       |
| Large Scale Processing   | A data protection impact assessment shall, in particular, be required in case of processing on a large scale of special categories of data.         |
| Involves New Technologies| A DPIA is welcomed when it involves the use of new (non-mature) technologies.                                                               |
| Concerns Vulnerable Individuals | A DPIA is welcomed when it concerns vulnerable individuals.                                                                                 |
| Difficult to Exercise Rights | A DPIA is welcomed when the controller cannot enable DS rights for technical or disproportionate effort reasons.                             |
| Involves Data Transfer Outside EU | A DPIA is welcomed when cross-border transfers are involved.                                                                                 |
| High Risk                | A DPIA is a must when the processing has a high residual risk.                                                                              |
| Imposed by Supervisory Authority | A DPIA can be requested by a supervisory authority.                                                                                         |
| Other                    | Other viable reason for conduction a thorough DPIA.                                                                                           |
**Transfer Contract Information class**: Summarizes the list of information to be provided when a cross-border data transfer is based on standard contractual clauses, agreements, or binding corporate rules.

| Literal                        | Description                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| **DPO Tasks**                 | A description of the DPO(s) tasks and responsibilities with regard to the data transfer and processing.                                      |
| **DPO Contact**               | The contact details of the involved DPS(s).                                                                                                    |
| **Compliance Procedures**     | A description of the technical and organizational measures and the procedures employed for ensuring and monitoring compliance.                |
| **Reporting Mechanisms**      | A description of the mechanisms for reporting and recording changes to the data transfer rules and reporting those changes to the supervisory authority. |
| **Personal Training**         | A description of the training that the employee involved in data transfer and processing have taken.                                          |
| **Other**                     | Any other information that is relevant to cross-border transfer rules.                                                                           |
| **Undertaking Structure**     | The structure and relationship of the undertakings that are involved in some common activities (cooperation).                                   |
| **Contact Details**           | The contact details of the groups of undertakings and each of its constituent members.                                                          |
| **Common Activities**         | A detailed description of the common activities carried out within the groups of undertakings.                                                   |
| **Specific Activities**       | A detailed description of the (non-common) activities of each undertaking involved in a group of undertakings.                                 |
| **Transfers Sequence**        | A complete description of data flow transfers, including all onward transfers and processing.                                                   |
| **D. Categories**             | A description of the concerned personal data categories.                                                                                    |
| **Type Proces. After Trans.** | A description of the type processing that will be applied on the personal data after transfer.                                               |
| **Purposes Processing After Trans.** | A description of the purpose of each processing that will be applied to the personal data after transfer.                               |
| **Type DS Affected**          | A description of the DS segment that is likely to be impacted by the transfer and subsequent processing.                                      |
| **Target Countries**          | A list of all countries and territories through which the data will flow.                                                                       |
| **I. Countries Binding Laws** | A description of all internal law bindings of the controllers and processors to which the data is disclosed.                                  |
| **E. Countries Bindings Laws** | A description of all relevant and enforceable laws of the countries and territories through which the data will flow.                         |
| **Applied GDPR Principles**  | A demonstration that all GDPR principles are being satisfied when transferring the data and when processing it afterward.                   |
| **Security Measures**         | A description of the security measures to safeguard data during and after the transfer.                                                        |
| **Onward Transfer Requirements** | A description of onward requirements for the transfer to bodies not bound by binding corporate rules.                                      |
| **Liability Sharing**         | A description of the responsibility and liability sharing between all actors that are involved in the transfer and processing.                |
| **How DS Informed**           | A clear description of how and when DS will be informed about the data transfer and subsequent processing.                                    |
Transfer Derogation Types class: Lists the standard situation where a cross-border data transfer is possible although it is not based on an adequacy decision, contractual clauses, agreements, nor binding corporate rules.

Table 25 Transfer Derogation Types class

| Literal                     | Description                                                                                                                                 |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Supported by Consent        | The DS has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards. |
| Necessary for Contact       | The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures where the DS is involved.       |
| Public Interest             | The transfer is necessary for important reasons of public interest.                                                                         |
| Exercise or Defence of Legal Claims | The transfer is necessary for the establishment, exercise or defense of legal claims.                                                  |
| Protect DS Vital Interests  | The transfer is necessary to protect the vital interests of the DS or of other persons, where the DS is physically or legally incapable of giving consent. |
| Public Consultation         | The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest. |
| Other                       | Other derogations that rely on the authorization of a supervisory authority are also possible.                                               |

SA Corrective Action Type class: Standard actions that a supervisory authority (SA) can apply on controller/processor.

Table 26 SA Corrective Action Type class

| Literal                     | Description                                                                                                                                 |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Warning                     | SA can issue a warning.                                                                                                                     |
| Reprimand                   | SA reprimand a controller.                                                                                                                  |
| Request Technical Update    | SA can order a technical update based on state of the art.                                                                                   |
| Request Organizational Update| SA can order a change in the organizational measures and procedures of the establishment.                                                     |
| Certification Withdrawal    | SA can withdraw a certification (involving administrative fines).                                                                          |
| Processing Suspension       | SA can order the temporary suspension of some processing.                                                                                     |
| Processing Ban              | SA can ban processing and order the destruction of data.                                                                                      |
| Administrative Fines        | SA impose administrative fines based on the infringement.                                                                                     |
| Other                       | Other corrective actions.                                                                                                                    |
Investigation Type class: Lists some common whys for supervisory authorities to conduct their investigations.

| Literal                  | Description                                                                 |
|--------------------------|-----------------------------------------------------------------------------|
| One Site Inspection      | Involves the inspection at the premises of the controller/processor, for example, to check the installation of a video surveillance system and the data retention period. |
| File Inspection          | Supervisory authorities’ subject controllers/processors to questionnaire and document request and review of answers and relevant documents. |
| Data Protection Audit    | A more general, complete and in-depth review of the relevant documentation.   |
| Other                    | Other type of investigations.                                               |

Infringement Type class: Some standard GDPR infringement that might give rise to administrative fines.

| Literal                  | Description                                                                 |
|--------------------------|-----------------------------------------------------------------------------|
| Principle Violation      | One or more GDPR principles were violated.                                  |
| DS Right Violation       | One or more GDPR principles were violated or not supported.                 |
| Obligation Violation     | Violation of the controller/processor obligations.                          |
| False Declaration        | Any false information transmitted to a supervisory authority.               |
| Unauthorized Transfer    | Cross-border data that has no legal justification according to GDPR.       |
| Forbidden Processing     | Processing of categories of personal data not included into the derogations that enable such processing. |
| Other International Law Violation | Violation of international laws and treaties other than GDPR.           |
| Insufficient Security Measures | Not enough safeguards and logistics were put to protect data and its free flow. |
| Corrective Action Violation | Non-compliance with order or request from the SA.                      |
| Child Consent Violation  | It lays down for the establishing consent for a child DS.                   |
| Certification Obligation Violation | Non-compliance to the commitments and obligations imposed by a certification body. |
| Cross-Boarder Transfer Violation | Non-compliance with the contractual rules that govern cross-border data transfers. |
| Other Local Law Violation | Violation of member state local laws.                                      |
| Other                    | Other non-common infringement.                                             |
**Glossary:** As follows, we present the GDPR-related terminology we use across the different models presented in this paper.

| Term                  | Description                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Personal Data         | Personal data means any information relating to an identified or identifiable natural person.                                                                                                               |
| Data subject          | A natural person whose personal data is processed by a controller or processor.                                                                                                                                 |
| Union Law             | Regulation (i.e. laws) of the European Union.                                                                                                                                                                |
| Directive             | A legislative act that sets out a goal that all EU countries must achieve through their own national laws.                                                                                                    |
| Controller            | A natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data where the purposes and means of such processing are determined by national or EU laws or regulations, the controller or the specific criteria for its nomination may be provided by national or EU law. |
| Processor             | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Moreover, data processors need to assist controllers in various circumstances where relevant, for example in a potential personal data breach notification or in considering a Data Protection Impact Assessment. |
| Processing            | Any operation performed on personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Identifiable natural person | An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Restriction of processing | It means the marking of stored personal data with the aim of limiting their processing in the future.                                                                                                      |
| Profiling             | It means to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.         |
| Pseudonymisation      | It means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. |
| Filing system         | It means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. |
| Recipient             | It means that a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. |
| Third party           | It means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. |
| Consent               | It means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| Personal data breach  | It means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. |
| Term                                    | Description                                                                                                                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Biometric data                         | It means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. |
| Data concerning health                 | It means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.                             |
| Representative                         | It means a natural or legal person established in the Union who, designated by the controller or processor.                                                                                                    |
| Enterprise                             | It means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.                                    |
| Group of undertakings                  | It means a controlling undertaking and its controlled undertakings.                                                                                                                                            |
| Supervisory authority                  | It means an independent public authority which is established by a Member State.                                                                                                                             |
| Relevant and reasoned objection        | It means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union. |
| International organization             | It means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.                                |
| Purpose                                | The purpose of data processing is said to be lawful if its legal basis matches one of the possible circumstances under which GDPR permits the processing of personal data. Example of valid legal basis for data processing are consent and when processing is necessary to perform or prepare for a contract with the data subject. |
| Member State Law                       | Specific regulation (i.e. laws) from a European member state.                                                                                                                                                 |
| Processing personal data collected for different purpose | Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent or on a Union or Member State law.                          |
| Encryption                             | Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.                                                              |
| Child                                  | Any identifiable natural person that is below of 16 years.                                                                                                                                                     |
| Special categories of personal data    | Special categories of personal data include: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited. |
| Criminal convictions and offenses data | Criminal convictions and offenses data represent personal data relating to criminal convictions and offenses or related security measures.                                                                       |
| Transparent information                | It means processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.                  |
| Right to rectification                 | The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.                                                   |
| Term                                      | Description                                                                                                                                                                                                 |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Right to be Forgotten                     | Also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data. |
| Right to restriction                      | The data subject shall have the right to obtain from the controller restriction of processing the data.                                                                                                        |
| Right to data portability                 | The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. |
| Right to object                           | The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her.                                                  |
| Right not to be subject to a decision     | The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. |
| Data Protection by Design                 | A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.                                                                               |
| Joint controllers                         | Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR regulation.                                                    |
| Personal data breach                      | It is a security incident in which information is accessed without authorization.                                                                                                                            |
| Data protection Impact Assessment          | A tool used to identify and reduce the privacy risks of entities by analyzing the personal data that are processed and the policies in place to protect the data.                                                |
| Legislative measures                      | They are laws, treaties and regulations on the protection of traditional knowledge and traditional cultural expressions, and legislative texts relevant to personal data.                                               |
| Data protection officer                    | A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. |
| Right to Access                           | Also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.                                              |
| Code of conduct                           | It is intended to contribute to the proper application of the GDPR taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. |
| Data protection certification             | It is meant to demonstrate compliance with the GDPR of processing operations by controllers and processors.                                                                                                      |
| Infringement                              | It is meant to the action of breaking the terms of the GDPR regulation.                                                                                                                                       |
| Cross-border data transfer                 | The GDPR permits personal data transfers to a third country or international organization subject to compliance with set conditions, including conditions for onward transfer.                                       |
| Standard Contractual Clauses              | They are a common, standardized method for transferring personal data to controllers and processors located in non-adequate countries outside of the EEA. These act as a contract between two legal entities and they do not require a license. |
| Binding Corporate Rules                   | They are internal rules which define the international policy in a multinational group of companies and international organizations regarding intra-organizational personal data cross-border transfers. |
| Term                        | Description                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Genetic data                | It means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. |
| Adequacy Decision           | An adequacy decision is a decision taken by the European Commission establishing that a third country provides a comparable level of protection of personal data to that in the European Union, through its domestic law or its international commitments.                                                                                                   |
| Data Controller             | A natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.                                                                                                                                                                           |
| Cross-border processing     | This type of processing often involves a unique multi-international controller/processor. Cross-border processing might take place in more than one Member State where the controller or processor is established. Cross-border processing might take place in the context of the activities of a single establishment of a controller or processor in the Union, but which substantially affects or is likely to substantially affect data subjects in more than one EU State. |
| Data Processing             | Is any operation performed on personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, etc.                                                                                                                                                   |
| Delegated Acts              | Non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity.                                                                                                                                                                                                                                                                         |
3 Constraints expressed in natural language.

As follows, we present the 35 compliance rules, in plain-English, we extracted from the GDPR.

### Table 33 Chapter I: General provisions

| ID | Source | Description |
|----|--------|-------------|
| C1 | Articles 2, and 3 | GDPR applies if some personal data is being processed or transferred AND The involved organizations are either operating within the EU OR operating outside the EU, but offering goods or services to individuals within the EU NEVERTHELESS GDPR does not apply for processing concerned with national security purposes OR processing covered by law enforcement directives OR processing carried out by individuals for personal/household activities |

### Table 34 Chapter II: Principles

| ID | Source | Description |
|----|--------|-------------|
| C2 | Article 5 | Each processing of personal data must demonstrate that it meets GDPR principles (Principles::Demonstration). |
| C3 | Article 6 | IF lawfulness is based on a legal obligation, THEN further information about the obligation need to be provided (Principles::Obligation Source) AND IF the processing is for a purpose other than that for which the personal data have been collected AND processing is not based on the data subject’s consent OR on a Union or Member State law, THEN additional information to demonstrate lawfulness are required (Principles::Lawfulness_Evidence). |
| C4 | Article 7 | All the Boolean attributes of DataProcessing:: Consent, which represent the requirement that a consent agreement must meet, should evaluate to true |
| C5 | Article 8 | When lawfulness is based on consent the DS must be at least 16 years old. OTHERWISE, the DS must be a child DS (Data Subjects::Child Data Subject) AND Consent for data child subject has to be provided by their legal responsible parent (Data Subjects::Responsible Parent) |
| C6 | Article 9 | Processing of Special data categories (all the enumeration in Enumerations::Data Category, except OTHER PERSONAL DATA) are prohibited unless the processing: is based on consent (if prohibition can be lifted by consent) OR is necessary for employment or social security OR is necessary to protect vital subject interest (consent is not possible) OR is based on legitimate activities carried by any legal not-for-profit body OR concerns data that are manifestly made public by the data subject OR is necessary for the establishment, exercise or defense of legal claims OR is necessary for reasons of substantial public interest OR is necessary for the purposes of preventive or occupational medicine OR is necessary for reasons of public interest in the area of public health OR is necessary for scientific, historical, research or statistical purposes OR allowed by Member state law |
| C7 | Article 10 | Processing based on consent that deals with criminal convictions AND offenses or related security measures shall be carried out only under the control of official authority or When the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights AND freedoms of data subjects AND Any comprehensive register of criminal convictions shall be kept only under the control of official authority |
| C8 | Article 11 | IF processing deals with data that cannot make DS identifiable, THEN processing does not have to enable DS personal rights such as the right of access |
Table 35 Chapter III: Rights of the data subject (1 of 2)

| ID  | Source  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C9  | Article 12 | Each processing of personal data must support DS rights when they are applicable AND Controllers have to react for a request to exercise a DS right within one month which can be extended by two further months where necessary, taking into account the complexity and number of the requests (DS must be informed of extension) AND IF the controller is not in a position to address a given requested DS right, THEN DS should be informed about the reasons related to this denial AND remind DS of his right to lodge a complaint AND DS right should be free of charge, UNLESS request unfounded or excessive (e.g., repetitive requests) AND A controller must verify the DS identity (might ask for further information for that purpose) |
| C10 | Article 13 | Where personal data relating is collected directly from DS, the controller shall, at the time when personal data are obtained, provide: the identity and contact details of the controller AND DPO contact details (if exists) AND purpose and lawfulness sources AND data recipients details (if exists) AND transfer to a third party and safeguards details (if applicable) AND storage duration AND DS enabled rights AND The right to withdraw consent (if exists) AND the right to lodge a complaint AND contractual requirements, e.g., mandatory and possible consequences of non-collaboration (if applicable) AND automated decision-making details (if applicable) AND details about any further processing (if applicable) UNLESS the DS is already informed |
| C11 | Article 14 | Where personal data is not directly collected from DS, the controller shall provide DS with the following information: The identity and contact details of the controller AND DPO contact details (if exists) AND Purpose and lawfulness sources AND Data categories and details about the data concerning the DS AND Data recipients details (if exists) AND Transfer to a third party and safeguards details (if applicable) AND Storage duration AND DS enabled rights AND The right to withdraw consent (if exists) AND The right to lodge a complaint AND Automated decision-making details (if applicable) AND Details about any further processing (if applicable) UNLESS the DS is already informed OR Providing information requires dispassionate effort OR collection is foreseen by law OR professional secrecy obligations |
| C12 | Article 15 | The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: Purpose and lawfulness sources AND Data recipients details AND Storage duration AND DS enabled rights AND The right to lodge a complaint AND Source of data (if collected indirectly) AND Automated decision-making details (if applicable) AND The right to receive a copy (free if first time) of personal data (UNLESS request affects rights and freedom of others) AND Appropriate safeguards in case of a cross-border transfer (if applicable) |
| C13 | Article 16 | Obligation to notify the rectification to each recipient to whom the data has been disclosed (unless disproportionate effort) AND Obligation to inform the DS of other recipients (if exists)                                                                                                                                                                                                                                                                 |
| C14 | Article 17 | The controller must satisfy the DS right to be forgotten when: the data are is no longer necessary OR the data subject withholds consent OR DS objects OR data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject OR consent or processing unlawful UNLESS the processing is necessary for: exercising the right of freedom of expression and information OR compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject OR the performance of a task carried out in the public interest OR the exercise of official authority vested in the controller OR public interest in the area of public health OR for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. IF triggered, other recipient and DS have to be informed |
| C15 | Article 18 | The data subject shall have the right to obtain restriction of processing when: the accuracy of the personal data is contested OR the processing is unlawful and the DS opposes the erasure of the personal data and requests the restriction of their use instead OR the controller no longer needs the personal data for the purposes of the processing, but they are required by the DS for the establishment, exercise or defense of legal claims OR the data subject has objected the processing and Notification obligation when the restriction is posed or is lifted |
### Table 36 Chapter III: Rights of the data subject (2 of 2)

| ID | Source | Description |
|----|--------|-------------|
| C16 | Article 20 | Data portability should be realized (upon request) when: the processing is not necessary for the performance of a task carried out in the public interest AND the processing is not necessary for the exercise of official authority vested in the controller AND DS identity verified AND technically feasible AND related lawfulness is based on consent or contract AND relevant data was directly collected from DS AND data portability does not affect the rights of all parties and laws OTHERWISE, the controller may deny the request (inform DS for reasons) |
| C17 | Article 21 | The DS shall have the right to object when processing purpose is for marketing OR The DS shall have the right to object when lawfulness is based on which is based on Consent OR legitimate interests OR public interest UNLESS controller demonstrates legitimate grounds which override the rights of DS, e.g., defense of legal claims. In any case, personal data shall no longer be processed for such purposes if objection accepted |
| C18 | Article 22 | The DS shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her UNLESS the automated decision is: is necessary for entering into, or performance of, a contract between the DS and a controller (but no special categories) OR is authorized by Union or Member State law to which the controller is subject OR is based on the DS’s explicit consent. |
| ID  | Source | Description                                                                                                                                                                                                 |
|-----|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C19 | Articles 24 and 25 | The controller shall implement appropriate technical and organizational measures, including data protection policies, to ensure and to be able to demonstrate that processing is performed in accordance with GDPR AND Implemented measures shall be reviewed and updated where necessary AND The controller shall adhere to Data protection by design and by default principle |
| C20 | Article 26 | Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR AND The responsibilities arrangement shall be made available to the data subject                                                   |
| C21 | Article 27 | When the controller or the processor is outside EU, it shall designate a representative in the Union UNLESS processing is occasional AND does not include processing of special categories of data and is unlikely to result in a risk to the rights and freedom of natural persons OR is consulted by a public authority or body AND IF a representative is designated, THEN it shall be established in one Member States |
| C22 | Articles 28 and 29 | A processor shall only act on the controller’s documented instructions or the processor shall inform the controller of any intended changes AND A processor shall check that there are no conflicts between the controller’s instructions and applicable EU law AND A processor shall ensure confidentiality AND A processor shall cooperate with supervisory authority AND A processor shall instore appropriate technical and organizational security measures AND A processor shall designate and collaborate with a DPA (when needed) |
| C23 | Article 30 | Controllers and their representatives shall record and maintain (in electronic form) processing activities, in particular: the name and contact details of the controller (or joint controllers), representatives and DPO (if applicable) AND the purposes of the processing AND a description of the categories of data subjects and of the categories of personal data AND the recipients to whom the personal data have been or will be disclosed AND where applicable, transfers of personal data to a third country or an international organization (+ the documentation of suitable safeguards) AND where possible, the envisaged time limits for erasure of the different categories of data AND where possible, a general description of the technical and organizational security measures Similarly, processors have to record: the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller’s or the processor’s representative, and the data protection officer AND the categories of processing carried out on behalf of each controller AND where applicable, transfers of personal data to a third country or an international organization (+ the documentation of suitable safeguards) AND where possible, a general description of the technical and organizational security measures. |
| C24 | Article 31 | The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks. |
Table 38 Chapter IV: Controller and processor (2 of 2)

| ID | Source       | Description                                                                                                                                                                                                 |
|----|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C25| Article 32   | The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including: the pseudonymisation and encryption of personal data AND the ability to ensure confidentiality, integrity, availability and resilience of processing systems and services AND the ability to restore the availability and access to personal data in the event of a physical or technical incident AND a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures |
| C26| Articles 33 and 34 | When data breaches are detected by a controller, the controller should act according to the associated risk: "Case low": record breaches "Case Medium": Case low + notify the concerned SA within 72 hours (any delay requires justification and might lead to administrative fines) "Case High": "Case Medium" + communication to DS without undue delay When data breaches are detected by a processor, the processor informs all involved controllers without undue delay after becoming aware of a personal data breach |
| C27| Article 35   | Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Is mandatory when: the processing is a systematic and extensive evaluation of personal aspects (e.g., profiling) or processing is used for automated decisions that might affect the natural person OR the processing is processing on a large scale of special categories of data OR the processing is a systematic monitoring of a publicly accessible area on a large scale OR type of processing is present in the list of processing types that must have a DPIA as published by SA OR Member state law requires processing without DPIA UNLESS the type of processing is present in the list of processing types that should no longer have a DPIA as published by SA OR similar DPIA exist (re-use measures) OR Member state law allows processing without DPIA AND The controller shall seek the advice of the data protection officer AND IF DPIA exists THEN, it should contain at least: A description of the processing and its purposes AND An assessment of the necessity and proportionality AND An assessment of the risks to individuals AND The measures in place to address risks, including security measures and compliance demonstration |
| C28| Article 36   | When a data protection impact assessment indicates that the processing would result in a high risk, the controller shall consult the supervisory authority prior to processing AND IF a consultation exists, THEN, The supervisory authority shall, within a period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller (period extensible to six weeks + notification) AND A controller shall provide all relevant information for communication |
| C29| Articles 37 and 38 | The designation of a DPA is mandatory when: The controller or processor is a public authority or body (except for courts acting in their judicial capacity) OR If processing concerns large scale systematic monitoring of individuals (e.g., online behavior tracking) OR large scale processing of special categories of data or data relating to criminal convictions and offenses |
| C30| Article 42   | The certification shall be voluntary and available via a process that is transparent AND A certification must be provided by an accredited body (accredited by an SA) AND A certification last three years AND A certification does not make controllers/processors less accountable |
### Table 39 Chapter V: Transfers of personal data to third countries or international organizations

| ID  | Source          | Description                                                                                                                                                                                                                                                                                                                                 |
|-----|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C31 | Articles 44, 45, 46, 49 and 50 | An across-border transfer, including onward ones, shall only be permitted IF the transfer: remains within EU OR is supported by an adequacy decision OR is supported by one of the following: (Approved binding corporate rules in case of a corporation OR Approved standard contractual clauses OR Authorized (by SA) provisions in administrative arrangements OR Approved code of conduct or certifications OR Authorized (by SA) Binding and enforceable instrument between public bodies) UNLESS, transfer is part of one of the following derogations: DS has explicitly consented to the proposed transfer, (DS must be informed of possible risks + does not apply to public authorities) OR Transfer is necessary for the performance of a contract (requested by DS or concluded in the interest of DS + does not apply to public authorities) OR Transfer is necessary to protect the DS vital interests (when DS is incapable of giving consent) OR Transfer is necessary for the establishment, exercise or defense of legal claims OR Transfer is necessary for reasons of public interest (recognized in Union law or in the law of the Member State) OR Transfer is necessary for the establishment, exercise or defense of legal claims OR Transfer is necessary for the purposes of legitimate interests pursued by the controller (SA and DSs must be informed) |
| C32 | Article 45 | IF the adequacy decision involves some additional requirements (e.g., partial adequacy requirement that covers a specific sector within a third country), THEN the importer of the data must provide evidence of the satisfaction of these requirements |
| C33 | Article 48 | Any legal decision from a third country requiring the disclosure of personal data may only be recognised or enforceable if decision based on an international agreement, such as a mutual legal assistance treaty |
| C34 | Article 47 | To be approved, a binding corporate rules: are legally binding and apply to and are enforced by every member concerned involved in a joint economic activity, including their employees; AND confer enforceable rights on DS AND included the following information: The structure and contact details of the group and of each of its members AND The categories of personal data, the type of processing and its purposes, the type of data subjects affected AND The third countries and their legally binding nature, both internally and externally AND The application of the general data protection principles AND The rights of data subjects in regard to processing and the means to exercise those rights AND The liability sharing in case of a breach or infringement AND The means used to communicate with data subjects AND The tasks of any DPO or any other person or entity in charge of data protection AND The mechanisms for ensuring the verification of compliance with the BCRs (e.g., audits and methods for ensuring corrective actions) AND The mechanisms for reporting and recording changes to the BCRs and reporting those changes to the SA AND The appropriate data protection training to personnel having permanent or regular access to personal data AND The cooperation and reporting mechanisms to be used with the SA (e.g., eBay and ArcelorMittal) |
| C35 | Article 83 | The total maximum administrative fine can cumulate up to Max(10.000.000 EUR, 2 % total world-wide annual turnover of preceding financial year) when: controllers or processors obligations are not fulfilled, e.g., non-compliance to the requirements for child consent OR the criteria for the certification are no longer met OR the monitoring body reports an infringement due to miss-application of code of conducts. The total maximum administrative fine can add up to Max(20.000.000 EUR, 4 % total world-wide annual turnover of preceding financial year) when the infringements concern the violation of: the basic principles for processing OR DS rights OR cross-border transfers of personal data rules OR any additional obligation imposed by Member states OR orders from an SA, for example, non-compliance to a temporary or definitive limitation on processing |
### 4 Variability Table

As follows, we present the 20 variation points we extracted from the GDPR.

| ID | Source | Description | How to resolve |
|----|--------|-------------|----------------|
| V1 | Article 8 | EMS law may provide for a lower age (…) provided that such lower age is not below 13 years | Add the V1 OCL constraint to the generic model and implement $V_{getMinimumAgeForDS}$ based on the EMS laws. |
| V2 | Article 8 | Checks that a given person is indeed the holder of parental responsibility over a given data subject according to the EMS law | Add the V2 OCL constraint to the generic model and implement $V_{checkParentDocuments}$ based on the EMS laws. |
| V3 | Article 9 | The processing of sensitive personal data is prohibited unless the data subject has given explicit consent (…), except where (…) EMS law provide that the prohibition (…) may not be lifted by the DS | Implement $V_{prohibitionCanBeLiftedByConsent}$ of the constraint $C_6$ based on the EMS laws. |
| V4 | Article 9 | EMS may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health | Add the V4 OCL constraint to the generic model and implement $V_{verifyFurtherConditionsAndLimit}$ based on the EMS laws. |
| V5 | Article 23 | EMS law (…) may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22, as well as Article 5 (…) when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society | Adapt the OCL constraints $C_2$, and from $C_9$ to $C_{22}$, that are already in the generic model, based on the restrictions of EMS laws. |
| V6 | Article 29 | The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by (…) EMS law | Implement $V_{processWithoutControllerInstructions}$ used in the constraint $C_{22}$ based on the EMS laws. |
| V7 | Article 32 | The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by (…) EMS law | Add the V7 OCL constraint to the generic model and implement $V_{processWithoutControllerInstructions}$ based on the EMS laws. |
| V8 | Article 36 | EMS shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information | Add the V8 OCL constraint to the generic model, RECONCILIATION_ASSESSMENT enumeration literal in DPIA.Information_Type, and implement $V_{ReconcileByLaw}$ based on the EMS laws. |
| V9 | Article 37 | In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by (…) EMS law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors | Implement $V_{bodiesMustDesignateDPO}$ used in the constraint $C_{29}$ based on the EMS laws. |
| ID | Source | Description | How to resolve |
|----|--------|-------------|----------------|
| V10 | Article 49 | In the absence of an adequacy decision, (...) EMS law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation | Add the V10 OCL constraint to the generic model and implement \( V_{\text{verifyTransferLimits}} \) based on the EMS laws. |
| V11 | Article 80 | EMS may provide that any body, organisation or association (...) has the right to lodge, in that MS, a complaint with the supervisory authority (...) and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed | Add the V11 OCL constraint to the generic model. |
| V12 | Article 83 | Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each EMS may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that EMS | Replace the C35 OCL constraint with the V12_1 OCL constraint, and add the V12_2 OCL constraint to the generic model. |
| V13 | Article 84 | MS shall lay down the rules on other penalties applicable to infringements of this Regulation | Add the V13 OCL constraint to the generic model. |
| V14 | Article 85 | Notwithstanding paragraph 1, EMS law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health | Add the V14 OCL constraint to the generic model. |
| V15 | Article 87 | EMS may further determine the specific conditions for the processing of a national identification number or any other identifier of general application | Add the V15 OCL constraint to the generic model, implement \( V_{\text{checkedIDProcessing}} \) based on the EMS laws, and add the IDENTIFICATION literal to the Data Category enumeration. |
| V16 | Article 88 | EMS may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context | Add the EMPLOYMENT_ASSESSMENT literal to the DPIA Information Type enumeration. |
| V17 | Article 89 | Where personal data are processed for scientific or historical research purposes or statistical purposes, (...) EMS law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 | Add the V17 OCL constraint to the generic model, and implement \( V_{\text{checkDerrogationsFromRights}} \) based on the EMS laws. |
| V18 | Article 89 | Where personal data are processed for archiving purposes in the public interest, (...) EMS law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 | Add the V18 OCL constraint to the generic model, and implement \( V_{\text{checkDerrogationsFromRights}} \) based on the EMS laws. |
| V19 | Article 90 | EMS may adopt specific rules to set out the powers of the supervisory authorities (...) in relation to controllers or processors that are subject, under (...) EMS law or rules established by national competent bodies, to an obligation of professional secrecy | Add the V19 OCL constraint to the generic model, and implement \( V_{\text{checkDerrogationsFromRights}} \) based on the EMS laws. |
| V20 | Article 91 | Where in a EMS, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation | Add the V20 OCL constraint to the generic model, and the CHURCH_REVOCATION literal to the Actor_Type enumeration. |
Appendix B

In this Appendix, we present the 35 compliance rules, presented in plain English in Section 3 of Appendix A, expressed in OCL.

1 context Data_Processing
2 def: getIdentifiableDS(dp:Data_Processing):Set(Data_Subject) = dp.personal_data.data_subject->flatten()->asSet()
3 inv C1:
4 processing->notEmpty()
5 and
6   processing.actors->exists(a|a.countries->exists(c|c.isEUMemberState or c.EULawApplies))
7 or processing->select(dp:Data_Processing|dp.type=OFFERING_GOODS_OR_SERVICES or dp.type=EU_BEHAVIOUR_MONITORING_OR_PROFILING)
8   ->exists(dp|getIdentifiableDS(dp).residence->exists(country|country.isEUMemberState or country.EULawApplies))
9 end
10
11 inv C2:
12 processing->forAll(p|p->select(demostrates->notEmpty()))
13
14 context Lawfulness
15 inv C3:
16 let processing: Set(Data_Processing)=Data_Processing.allInstances()->select(personal_data->notEmpty()),
17 legal_obligation_lawfulness:Set(Lawfulness)=Lawfulness.allInstances()->select(l|l.Lawfulness_Source.source=LEGAL_OBLIGATION) in
18 if (legal_obligation_lawfulness->notEmpty())
19 then
20 legal_obligation_lawfulness->forAll(l:Lawfulness|l.Lawfulness_Source->forAll(ls|ls.obligation_source.moreInformation<>)
21 )
22 else false
23 endif
24
25 inv C4:
26 Consent.allInstances()->forAll(c| c.isFreelyGiven
27 and c.canBeWithdrawn
28 and c.unambiguous
29 and c.involvesConfirmationAction
30 and c.distinguishableFromOther
31 and c.isIntelligible
32 and c.isEasyToAccess
33 and c.usesClearPlainLanguage
34 and c.describeSubjectEnabledRights
35 and c.isEasyToWithdraw)
36
37 inv C5:
38 self.isLawfulnessOnlyByConsent() implies
39 let identifiableSubjects : Set(Data_Subject) = self.personal_data.data_subject->flatten()->asSet() in
40 self.purposes->forAll
41 (p:Purpose|
42 identifiableSubjects->forAll(ds:Data_Subject|
43 let eligibleToFoGiveConsent : Natural_Person =
44 if ds.oclIsTypeOf(Data_Subject)
45 )
9     if ds
10     else ds.getResponsibleParent()
11     endif in p.getConsents()->exists(c:Consent|
12       c.provider=eligibleToGiveConsent
13       and c.target=ds
14     )
15   )
16   )

inv C6:
2   processing->forall(dp:Data_Processing|dp.personal_data->forAll(pd|
3     if (Bag{Data_Category::RACIAL_OR_ETHNIC, Data_Category::RELIGIOUS_OR_PHILISOPHICAL_BELIFS, Data_Category::
4       POLITICAL_OPINIONS, Data_Category::HEALTH, Data_Category::SEX_LIFE, Data_Category::GENETIC, Data_Category::
5       BIOMETRIC, Data_Category::JUDICIAL})->includes(pd.category)
6     and not dp.purposes->forAll(p|
7       if Variability.V_prohibitionCanBeLiftedByConsent(dp)
8       then p.consent->notEmpty()
9       else false
10      endif
11     or Bag{Processing_Context::EMPLOYMENT, Processing_Context::VITAL_INTERESTS, 
12       Processing_Context::SHARED_BY_DATA_SUBJECT, Processing_Context::STATISTICAL_PURPOSES, 
13       Processing_Context::RESEARCH, Processing_Context::LEGAL_AND_CRIMINAL_INVESTIGATION, 
14       Processing_Context::PUBLIC_INTEREST, Processing_Context::PREVENTIVE_MEDICINE, 
15       Processing_Context::PUBLIC_HEALTH})->includes(p._context)
16     or p.hasLegitimateInterest))
17     then isForbidden=true
18     else isForbidden=false
19   endif)

inv C7:
2   processing->forall(dp |
3     if dp.Lawfulness_Source.source = BY_CONSENT and dp.purposes -> exists(p | p._context = 
4       LEGAL_AND_CRIMINAL_INVESTIGATION) and(dp.security_measure -> notEmpty()) then 
5     dp.getConcernedSupervisoryAuthority().type = Actor_Type::OFFICIAL
6     else false
7   endif)

inv C8:
2   processing->forall(dp |
3     if dp.areDataSubjectIdentifiable then dp.right - > isEmpty()
4     else false
5   endif)

inv C9:
2   processing->forall(dp|dp.right->notEmpty())
3   and
4   Data_Controller.allInstances()->forall(dc|
5     if dc.Contract_Agreement.duration() < 1 then 
6     true
7     else if (dc.Contract_Agreement.duration() >= 1 and dc.Contract_Agreement.duration() <=3) then 
8     dc.Contract_Agreement.data_processing->forall(dp|dp.right->
9       select(oclIsKindOf(Right_To_Be_Informed))->forall(r|r.oclAsType(Right_To_Be_Informed).
10       informDS())
11     )
12     else false
13     endif
14   endif
15   )
16   and
17   Data_Controller.allInstances()->forall(dc|
18     if dc.rightNotAddressed()<null then 
19     dc.Contract_Agreement.data_processing->forall(dp|dp.right
20     ->select(oclIsKindOf(Right_To_Be_Informed))
21     ->forall(r|
22     r.oclAsType(Right_To_Be_Informed).information
23     ->exists(i|i.type=Information_Type::RIGHT_TO_LODGE_COMPLAINT

inv C10:
def:data_controllers(dp : Data_Processing) : Set(Actor) = dp.actors->select(a|a.oclIsTypeOf(Data_Controller))
def:processing_related_to_controller (actor:Actor) : Set(Data_Processing) = actor.oclAsType(Data_Controller).Contract_Agreement.data_processing

inv C11:
processing->forAll(dp)

if (dp.operation=COLLECTING) then (dp.personal_data->forAll(pd)
if pd.collectedDirectly then (data_controllers(dp)->forAll(actor)
processing_related_to_controller(actor)->forAll(dp|dp.right->select(oclIsKindOf(Right_To_Be_Informed)))
->forAll(r)
let right:Right_To_Be_Informed=r.oclAsType(Right_To_Be_Informed) in
if not right.DSAlreadyInformed then
let actual_info:Bag(Information_Type)=right.information->collect(i|i.type) in
actual_info->includes(Bag
Information_Type::CONTROLLER_DETAILS, Information_Type::DPO_DETAILS, Information_Type::PURPOSE_AND_LAWFULNESS, Information_Type::RECIPIENTS, Information_Type::TRANSFERRED_TO_THIRD_COUNTRIES, Information_Type::STORAGE_DURATION, Information_Type::DS_RIGHTS, Information_Type::CONSENT_WITHDRAWABLE, Information_Type::RIGHT_TO_Lodge_COMPLAINT, Information_Type::STATUTORY_CONTRACTUAL_REQUIREMENT, Information_Type::AUTOMATED_DECISION, Information_Type::FURTHER_PROCESSING)
else false
endif
)
else false
endif
)
else false
endif
)
let actual_info:Bag(Information_Type)=right.information->collect(i|i.type) in

actual_info->includes(Bag{
  Information_Type::CONTROLLER_DETAILS,
  Information_Type::DPO_DETAILS,
  Information_Type::PURPOSE_AND_LAWFULNESS,
  Information_Type::DATA_CATEGORIES,
  Information_Type::CONTACT_DETAILS,
  Information_Type::RECIPIENTS,
  Information_Type::TRANSFERS_THIRD_COUNTRIES,
  Information_Type::STORAGE_DURATION,
  Information_Type::DS_RIGHTS,
  Information_Type::CONSENT_WITHDRAWABLE,
  Information_Type::RIGHT_TO_Lodge_COMPLAINT,
  Information_Type::AUTOMATED_DECISION,
  Information_Type::FURTHER_PROCESSING
})

else false
endif

inv C12:
processing->forAll(dp|
  dp.personal_data->forAll(pd|
    data_controllers(dp)->forAll(actor|
      processing_related_to_controller(actor)->forAll(dp|
        dp.right->select(oclIsKindOf(Right_To_Access))
        ->forAll(r|
          let actual_info:Bag(Information_Type)=r.oclAsType(Right_To_Access).information->
          collect(i|i.type) in
            actual_info->includes(Bag{
              Information_Type::PURPOSE_AND_LAWFULNESS,
              Information_Type::RECIPIENTS,
              Information_Type::STORAGE_DURATION,
              Information_Type::DS_RIGHTS,
              Information_Type::RIGHT_TO_Lodge_COMPLAINT,
              Information_Type::DATA_SOURCE,
              Information_Type::AUTOMATED_DECISION
            })
          and r.oclAsType(Right_To_Access).impactsFreedomOfOthers implies
            actual_info->includes(Information_Type::RIGHT_TO_RECEIVE_COPY)
          and dp.isCrossBorders implies
            actual_info->includes(Information_Type::TRANSFERS_THIRD_COUNTRIES)
        )
      )
    )
  )
)

inv C13:
Right_To_Rectification.allInstances() ->
forAll(r | r.isRectification implies
  if not r.requiresDisproportionateEffort then r.notification -> forAll(n | n.recipient ->
    notEmpty() and r.informDS())
  else false
endif
)
inv C14:
Right_To_Erasure.allInstances()->forAll(
  rte| let processing_is_not_necessary: Boolean=rte->collect(r|r.reason)
  ->select(r1|r1=Denial_Erasure_Reason::FREEDOM_EXPRESSION_INFORMATION or
    r1=Denial_Erasure_Reason::COMPLIANCE_LEGAL_OBLIGATION or
    r1=Denial_Erasure_Reason::PUBLIC_INTEREST or
    r1=Denial_Erasure_Reason::ARCHIVING_PURPOSES or
    r1=Denial_Erasure_Reason::DEFENCE_LEGAL_CLAIMS)->isEmpty() in
  processing_is_not_necessary
  implies
  rte.denied=true
  and
  rte->collect(r|r.denialReason)->includes ( Erasure_Right_Reason::DATA_NO_LONGER_NECESSARY,
    Erasure_Right_Reason::CONSENT_WITHDRAWN,
    Erasure_Right_Reason::DS_OBJECTS,
    Erasure_Right_Reason::LEGAL_OBLIGATION,
    Erasure_Right_Reason::UNLAWFUL_PROCESSING)
  and
  rte.notification->forAll(n|n.recipient->notEmpty() and rte.informDS())
)

inv C15:
processing->forAll(dp|
  dp.personal_data->forAll(pd|
    data_controllers(dp)->forAll(actor|
      processing_related_to_controller(actor)->forAll(dp|
        dp.right->select(oclIsKindOf(Right_To_Restriction))
        ->forAll(r|
          Set{ Restriction_Right_Reason::CONTESTED_ACCURACY,
            Restriction_Right_Reason::UNLAWFUL_PROCESSING,
            Restriction_Right_Reason::DATA_NO_LONGER_NECESSARY,
            Restriction_Right_Reason::DS_OBJECTS
          }->includes(r.oclAsType(Right_To_Restriction).reason)
        )
      )
    )
  )
)

inv C16:
Right_To_Data_Portability.allInstances() -> forAll(rtdp |
  if (rtdp.data_processing ->
    forAll(dp | dp.purposes._context <> Processing_Context::PUBLIC_INTEREST and
      dp.areDataSubjectIdentifiable and(dp.Lawfulness_Source.source =
        Lawfulness_Source::BY_CONSENT or dp.Lawfulness_Source.source =
        Lawfulness_Source::PERFORMANCE_OF_CONTRACT)) and rtdp.checkIfPossible() and
    rtdp.data_processing -> forAll(dp | dp.personal_data.collectedDirectly = true) and not
    rtdp.affectRightsOfOthers)
  then rtdp.transferData() = true
  else rtdp.transferData() = false
endif)

inv C17:
Right_To_Object.allInstances() -> forAll(rto|
  if ( rto.data_processing ->
    forAll(dp | dp.Lawfulness_Source.lawfulness_evidence->select(le|le.specialCategoryEnabler=
      ESTABLISHMENT_EXERCISE_OR_DEFENSE_LEGAL_CLAIMS)->size()=0
    and (dp.purposes._context=Processing_Context::MARKETING or
      Bag{ Lawfulness_Source::BY_CONSENT, Lawfulness_Source::LEGITIMATE_INTERESTS,
        Lawfulness_Source::PUBLIC_INTEREST
      }->exists(dp.Lawfulness_Source.source)
    )
  )
)
14 )
15 )
then rto.object() = true
17 else rto.object() = false
18 endif
19 )

1 inv C18:
2 Right_To_Not_Be_Part_Of_A_Decision.allInstances() ->forall(right|
3 right.data_processing ->forall(dp|)
4 let nAutomatedPurposes = dp.purposes ->collect(p:Purpose|p._context = Information_Type::AUTOMATED_DECISION) ->size() in
5 if (%
6 dp.purposes ->size() = nAutomatedPurposes
7 and not dp.purposes ->forall(p|%
8 if (%
9 p._context = Information_Type::AUTOMATED_DECISION
10 and dp.contractAgreement ->notEmpty()
11 and not dp.targetsSpecialDataCategories
12 )
13 then true
14 else false
15 endif
16 )
then right.object() = true
18 else right.object() = false
20 endif
21 )
22 )

1 inv C19:
2 processing ->forall(dp:Data_Processing|)
3 let measures = dp.security_measure,
4 technicalMeasures = dp.security_measure ->collect (sm | sm.oclIsTypeOf(Organizational)),
5 organizationalMeasures = dp.security_measure ->collect (sm | sm.oclIsTypeOf(Technical)) in
6 technicalMeasures ->notEmpty()
7 and organizationalMeasures ->notEmpty()
8 and organizationalMeasures ->exists(om | om.oclAsType(Organizational).type = Technical_Measure_Type::DATA_PROTECTION)
9 and measures ->forall(isRevisedPeriodically)
10 )

1 inv C20:
2 Joint_Controllers.allInstances() ->forall(jc | jc.responsibilitiesArrangement ->notEmpty() and jc.
3 arrangementMadeAvailableToDS)

1 inv C21:
2 processing ->forall(dp|)
3 let controller_or_processor_is_outside_EU: Set(Actor) = dp.actors ->
4 select(a | a.oclIsKindOf(Controller) or a.oclIsKindOf(Processor) and a.countries ->exists(c:Country|c.
5 isEUMemberState)) in
6 if (controller_or_processor_is_outside_EU ->notEmpty()%
7 and not dp.isOccasional
8 )
9 and (%
10 not (dp.targetsSpecialDataCategories)
11 or dp.actors ->exists(oclIsKindOf(Legal_Authority))
12 )
then controller_or_processor_is_outside_EU ->forall(a | a.oclAsType(Representative) <> null)
13 else false
14 endif
15 )
inv C22:
  processing->forAll(dp:Data_Processing|
    processors(dp)->forAll(a|
      let processor = a.oclAsType(Data_Processor) in
        not Variability.V.processWithoutControllerInstructions(dp, processor)
      implies (if processor.actedOnControllerDocumentedInstructions(dp) = true
        then true
        else processor.informedTheControllerOfIntendedChanges(dp) = true
        endif)
    and dp.actors->select(a|a.oclIsKindOf(Data_Controller))
    ->forAll(c|processor.checkedNoConflicts(c.oclAsType(Data_Controller)))
    and processor.ensuredConfidentiality
    and processor.cooperatedWithSA(dp)
    and (let measures=dp.security_measure->collect (sm|sm.oclIsTypeOf(Organizational)),
      organizationalMeasures=dp.security_measure->collect (sm|sm.oclIsTypeOf(Technical)) in
      technicalMeasures->notEmpty()
      and organizationalMeasures->notEmpty())
    and processor.data_protection_officer->notEmpty()
    ))

inv C23:
  processing->forAll(dp:Data_Processing|
    controllers(dp)->forAll(a|
      let controller = a.oclAsType(Controller),
      activity = controller.processing_activity,
      details = activity->collect(details) in
      activity->forAll(a|a.isElectronic)
      and details->includes
        (Bag{
          Information_Type::CONTROLLER_NAME,
          Information_Type::CONTROLLER_DETAILS,
          Information_Type::DPO_DETAILS,
          Information_Type::PROCESSING PURPOSES,
          Information_Type::DS CATEGORIES,
          Information_Type::PERSONAL_DATA_CATEGORIES,
          Information_Type::RECIPIENTS
        })
    and processors(dp)->forAll(a|
      let processor = a.oclAsType(Processor),
      proc_activities = processor.processing_activity,
      proc_details = proc_activities->collect(details) in
      proc_details->includes
        (Bag{
          Information_Type::PROCESSOR_NAME,
          Information_Type::PROCESSORS DETAILS,
          Information_Type::DPO DETAILS
        })
    and processor.actingAsControllers->forAll(a|
      proc_details->includes(ac.proc_activities->collect(details))
    )
    and let rep_activities = processor.representative.processing_activity in
    proc_activities->includes(rep_activities->collect(details))
    and proc_activities->forAll(a|
      a.transfersToThirdCountries implies a.details->exists(Information_Type::TRANSFERS THIRD COUNTRIES)
      and a.areErasureTimeLimitsKnown implies a.details->exists(Information_Type::TIME LIMITS FOR ERASURE)
      and a.areSecurityMeasuresKnown implies a.details->exists(Information_Type::SECURITY MEASURES)
    )
  )
  def:controllers(dp:Data_Processing) = Set(Actor) = dp.actors->select(a|a.oclIsKindOf(Controller))
inv C24:
processing->forAll(dp|
dp.actors->select(a|a.oclIsKindOf(Processor)
or a.oclIsKindOf(Controller)
or a.oclIsKindOf(Representative))
)->forAll(a:a.legal_authority->notEmpty())
)

def:main_intervenants (dp:Data_Processing) : Set(Actor) = dp.actors->select(a|a.oclIsTypeOf(Main_Intervenant))
inv C25:
processing->forAll(dp|
let organizational_measures = dp.security_measure->select(sm|sm.oclIsTypeOf(Organizational)),
technical_measures= dp.security_measure->select(sm|sm.oclIsTypeOf(Technical)) in
main_intervenants(dp)->forAll(a|
let appropriate_measures = a.oclAsType(Main_Intervenant).getAppropriateSecurityMeasures(dp) in
dp.security_measure->collect(type)->includes(appropriate_measures)
and technical_measures->collect(type)->includes(Bag{Technical_Measure_Type::PSEUDOANONYMIZATION,
Technical_Measure_Type::ENCRYPTION})
)
and main_intervenants(dp)->forAll(a|
let intervenant =oclAsType(Main_Intervenant) in
intervenant.ensuredPrinciples(dp)->includes(Bag{Integrity_And_Confidentiality,Availability, Resilience})
and
intervenant.canRestorePersonalData
and
intervenant.evaluatedMeasuresRegularly
)

inv C26:
processing->forAll(dp|dp.breach->
forAll(b|
let detector:Main_Intervenant = b.detectedBy in
detector.oclIsTypeOf(Controller)
implies (let controller=detector.oclAsType(Controller) in
Bag{Risk_Severity::LOW,Risk_Severity::MEDIUM,Risk_Severity::HIGH}->includes(b.severity)
implies controller.recordBreach(b)
and Bag{Risk_Severity::MEDIUM,Risk_Severity::HIGH}->includes(b.severity)
implies controller.notifyBreachToSA(b,controller.getConcernedSA(dp))<72
and Risk_Severity::HIGH = b.severity
implies personal_data.data_subject->flatten()->asSet()->forAll(ds|controller.notifyBreachToDS(b,ds)))
and detector.oclIsTypeOf(Processor)
implies detector.oclAsType(Processor).notifyBreachToAllControllers(b,dp)
)
)

inv C27:
processing->forAll(dp|
let dpias:Set(Data_Protection_Impact_Assessment) = dp.data_protection_impact_assessment in
dp.risk->exists(r|r.severity=Risk_Severity::HIGH
or r.impactsOnDS<>"
or dpias->exists(dpi:Data_Protection_Impact_Assessment|dpi.dpia_motivation->exists
(m.motivation=Enumerations::DPIA_Motivation::HIGH_RISK)
)) implies
controllers(dp)->forAll(c|c.oclAsType(Controller).assessProcessingImpact(dp))
and dpias->notEmpty()
and
(dp.operation=Operation_Type::PROFILING
or dp.purposes->includes(Processing_Context::BEHAVIOUR_MONITORING_OR_PROFILING)
or dpia->exists(dpia:Data_Protection_Impact_Assessment|dpia.dpia_motivation->exists(dm.dm.motivation=Enumerations::DPIA_Motivation::PROFILING))
)
implies dpias->forAll(isMandatory)
and
dp.purposes->includes(Processing_Context::TAKE_AUTOMATED_DECISIONS)
and
(dp.targetsSpecialDataCategories
   and dpias->exists(dpia|dpia.dpia_motivation->exists(dm|dm.motivation=Enumerations::DPIA_Motivation::LARGE_SCALE_PROCESSING))
)
   implies dpias->forAll(isMandatory)
and
dpias->exists(dpia|dpia.dpia_motivation->exists(dm|dm.motivation=Enumerations::DPIA_Motivation::SYSTEMATIC_MONITORING))
   implies dpias->forAll(isMandatory)
and
let mustHaveTypes:Set(Processing_Context)= mustHaveDPIA(dp.getConcernedSupervisoryAuthority().oclAsType(Supervisory_Authority)) in
dp.purposes->exists(p|mustHaveTypes->includes(p._context))
and
dpias->forAll(areInvolvedProcessingSimilar implies dpias->forAll(not isMandatory))
and
if dpias->notEmpty()
then
dpias->forAll(dpia|dpia.data_processing->notEmpty() and dpia.data_processing->forAll(not dp.type.oclIsUndefined()))
   and dpias->forAll(dpia|dpia.dpia_information->forAll(di:DPIA_Information|
      if (di.type=DPIA_Information_Type::RISK_ASSESSMENT
         and let tokens = di.summary.toLowerCase().tokenize(" ") in
            tokens->includes("high")
         )
      then dpia.Consultation->forAll(isMandatory)
      else false
      )
   )
else false
endif
})

inv C28:
processing->forAll(dp|
   dp.data_protection_impact_assessment->forAll(dpia:Data_Protection_Impact_Assessment|
      dpia.dpia_information->forAll(di:DPIA_Information|
         if (di.type=DPIA_Information_Type::RISK_ASSESSMENT
            and let tokens = di.summary.toLowerCase().tokenize(" ") in
               tokens->includes("high")
         )
         then dpia.Consultation->forAll(isMandatory)
         else false
      )
   )
)

def: controllers(dp: Data_Processing): Set(Actor) = dp.actors->select(a | a.oclIsKindOf(Controller))

inv C29:
processing->forAll(dp|
   let controllers:Set(Actor) = controllers(dp),
   processors:Set(Actor) = processors(dp) in
   if (controllers->union(processors)->exists(a|
      a.type=Actor_Type::PUBLIC_ORGANIZATION
      and (a.oclIsKindOf(Legal_Authority)
      or a.oclIsKindOf(Accreditation_Body)
      or a.oclIsKindOf(Certification_Body))
   and not a.oclIsKindOf(Court))
   )
   )
45

or
dp.purposes->exists(p|
  p._context=Processing_Context::BEHAVIOUR_MONITORING OR_PROFILING
or dp.data_protection_impact_assessment->exists(dpia|
  let dpia_motivations = dpia.dpia_motivation in
  dpia_motivations->includes(Bag{LARGE_SCALE_PROCESSING, SYSTEMATIC_MONITORING})
  or
dpia_motivations->includes(Bag{LARGE_SCALE_PROCESSING, INVOLVES_SPECIAL_OR.CRIMINAL_DATA})
))

then controllers->union(processors)->forAll(designates->size()=1)
else controllers->union(processors)->forAll(designates->size()>=0)
endif

inv C30:
Certification.allInstances()->forAll(cert: Certification |
  cert.isVoluntary and cert.isAvailableViaTransparentProcess and not cert.legal_authority ->
  isEmpty() and cert.validity = 3
)

inv C31:
Supervisory_Authority.allInstances()->forAll(
sa:Supervisory_Authority|sa.approved_legal_basis.data_transfer->forAll(
  dt:Data_Transfer|
  if
dt.IsWithinEU
  or dt.adequacy_decision->notEmpty()
  or dt.legal_basis->exists(lb|
    lb.oclIsTypeOf(Binding_Corporate_Rules)
  or lb.oclIsTypeOf(Standard_Contractual_Clauses)
  or lb.oclIsTypeOf(Administrative_Arrangement)
  or lb.oclIsTypeOf(Certification))
  or dt.code_of_conduct.isApproved=true
  and not (let transfer_derrogations = dt.legal_basis->select(oclIsTypeOf(Transfer_Derogation)) in
    Bag(
      Transfer_Derogation_Types::SUPPORTED_BY_CONSENT,
      Transfer_Derogation_Types::NECESSARY_FOR_CONTRACT,
      Transfer_Derogation_Types::PROTECT_DS_VITAL_INTERESTS,
      Transfer_Derogation_Types::DEFENCE_OFLEGAL_CLAIMS,
      Transfer_Derogation_Types::PUBLIC_INTEREST,
      Transfer_Derogation_Types::PUBLIC_CONSULTATION
    )->includes(transfer_derrogations)
    or transfer_derrogations->exists(let td = oclAsType(Transfer_Derogation) in
      not td.isTransfertRepetitive implies td.limitedNumberOfConcernedDS)
  )
then dt.isForbidden = false
else dt.isForbidden = true
endif
)

inv C32:
Data_Transfer.allInstances()->forAll(dt |
  let additional_requirements: Set(String) =
    dt.adequacy_decision.additionalRequirements->flatten()->asSet() in
    not dt.adequacy_decision.oclIsUndefined() and additional_requirements->forAll(
      requirement: String | requirement <> ""
    )
  implies dt.importer.provideEvidence(additional_requirements)->exists(dt.Adequacy_Evidence)
)

inv C33:
Data_Transfer.allInstances()->forAll(dt|
  if dt.adequacy_decision.basedOnInternationalAgreement
  and dt.adequacy_decision.country->exists(not isEUMemberState)
and dt.adequacy_decision.requiresDisclosureOfPersonalData
then dt.adequacy_decision.mayBeRecognised = true
and dt.adequacy_decision.mayBeEnforceable = true
else dt.adequacy_decision.mayBeRecognised = false
and dt.adequacy_decision.mayBeEnforceable = false
endif

inv C34:
Supervisory_Authority.allInstances().approved_legal_basis->collect(oclIsKindOf(Binding_Corporate_Rules))->forAll(lb |
let bcr = lb.oclAsType(Binding_Corporate_Rules) in
bcr.areLegallyBinding
and bcr.areEnforcedToEveryMember and bcr.applyToEveryMember and
bcr.conferEnforceableRightsOnDS and bcr.contract_information.type->includes(
Bag {
Transfer_Contract_Information::UNDERTAKINGS_STRUCTURE,
Transfer_Contract_Information::CONTACT_DETAILS
}) and bcr.contract_information.type->includes(
Bag {
Transfer_Contract_Information::DATA_CATEGORIES,
Transfer_Contract_Information::TYPE_PROCESSING_AFTER_TRANSFER,
Transfer_Contract_Information::PURPOSES_PROCESSING_AFTER_TRANSFER,
Transfer_Contract_Information::TYPE_DS_AFFECTED
}) and bcr.contract_information.type->includes(
Bag {
Transfer_Contract_Information::TARGET_COUNTRIES,
Transfer_Contract_Information::INTERNAL_COUNTRIES_BINDING_LAWS,
Transfer_Contract_Information::EXTERNAL_COUNTRIES_BINDING_LAWS
}) and bcr.contract_information.type->
includes(Transfer_Contract_Information::APPLIED_GDPR_PRINCIPLES) and
bcr.data_transfer.right->select(r | r.oclIsTypeOf(Right_To_Be_Informed))->notEmpty()
and bcr.data_transfer.breach->notEmpty() implies bcr.contract_information.type->
includes(Transfer_Contract_Information::LIABILITY_SHARING) and
bcr.contract_information.type->includes(Bag {
Transfer_Contract_Information::HOW_DS_INFORMED,
Transfer_Contract_Information::DPO_TASKS,
Transfer_Contract_Information::REPORTING_MECHANISMS,
Transfer_Contract_Information::REPORTING_MECHANISMS,
Transfer_Contract_Information::PERSONAL_TRAINING
})
)

inv C35:
Corrective_Action.allInstances()->forAll(ca: Corrective_Action |
(ca.type = SA_Corrective_Action_Type::ADMINISTRATIVE_FINES
and(ca.main_intervenant.obligation -> exists(obligation: Obligation | not
obligation.isFulfilled) or ca.infringement.type ->
exists(Infringement_Type::CHILD_CONSENT_VIOLATION) or ca.infringement.type ->
exists(Infringement_Type::OBLIGATION_VIOLATION) or ca.infringement.type ->
exists(Infringement_Type::CERTIFICATION_OBLIGATION_VIOLATION) or ca.infringement.type ->
exists(Infringement_Type::CODE_OF_CONDUCTS_MISS_APPLICATION))
implies ca.main_intervenant -> forAll(mi |
ca.TotalFines = 0.02 * mi.annualRevenue or ca.TotalFines <= 10000000) and(
ca.type = SA_Corrective_Action_Type::ADMINISTRATIVE_FINES and(
ca.infringement.type -> exists(Infringement_Type::PRINCIPLE_VIOLATION) or
ca.infringement.type -> exists(Infringement_Type::DS_RIGHT_VIOLATION) or
c.a.infringement.type -> exists(Infringement_Type::CROSS_BORDER_TRANSFER_VIOLATION) or
ca.main_intervenant.addionalObligations -> exists(ob | not ob.isFulfilled) or
c.a.infringement.type -> exists(Infringement_Type::OTHER_LOCAL_LAW_VIOLATION)
)
implies ca.main_intervenant -> forAll(mi |
c.a.TotalFines = 0.04 * mi.annualRevenue or ca.TotalFines <= 20000000)
)
Appendix C

In this Appendix, we present the resolutions (including new OCL constraints, if needed) of the 20 variation points discussed in Section 4 of Appendix A.

**V1 resolution:** Add V1 and implement V_getMinimumAgeForDS

```ocl
context Data_Subject inv V1:
let minDSAge: Integer = Variability.V_getMinimumAgeForDS(self) in
if (self.oclIsTypeOf(Child_Data_Subject))
then self.getAge() < minDSAge
else self.getAge() >= minDSAge endif
```

**V2 resolution:** Add V2 and implement V_checkParentDocuments

```ocl
context Natural_Person inv V2:
self.children->forAll(c:Child_Data_Subject|self.V_checkParentDocuments(c)
) )
```

**V3 resolution:** Implement V_prohibitionCanBeLiftedByConsent used in C6

**V4 resolution:** Add V4, implement V_verifyFurtherConditionsAndLimit

```ocl
inv V4:
processing->forAll(dp: Data_Processing | dp.personal_data->forAll(pd |
Bag {
  Data_Category::HEALTH, Data_Category::GENETIC, Data_Category::BIOMETRIC
  ) -> includes(pd.category) implies Variability.V_verifyFurtherConditionsAndLimit(dp = true)
})
```

**V5 resolution:** (1) Adapt C2, and (2) Adapt from C9 to C22

**V6 resolution:** Implement V_processWithoutControllerInstructions, used in C22

**V7 resolution:** Add V7 and implement V_processWithoutControllerInstructions

```ocl
inv V7:
processing->forAll(dp: Data_Processing |
dp.actors->select(a | a.type = Actor_Type::NATURAL_PERSON and a.actsUnderAuthorityOf->notEmpty())->forAll(np | Variability.V_processWithoutControllerInstructions(dp, np) implies np.actedOnControllerDocumentedInstructions(dp) = false)
}
```

**V8 resolution:** Add V8, and RECONCILIATION_ASSESSMENT enumeration literal in DPIA_Information_Type, and implement V_ReconcileByLaw

```ocl
inv V8:
processing->forAll(dp | Variability.V_ReconcileByLaw(dp) implies dp.data_protection_impact_assessment.dpia_information->collect(type)->includes(DPIA_Information_Type::RECONCILIATION_ASSESSMENT)
)
```

**V9 resolution:** Add V10 and implement V_verifyTransferLimits

```ocl
inv V10:
Supervisory_Authority.allInstances()->forAll(sa : Supervisory_Authority |
sa.approved_legal_basis.data_transfer->forAll(dt : Data_Transfer |
(Variability.V_limitTransfers() and dt.adequacy_decision->isEmpty() and dt.purposes->exists(p | p._context = PUBLIC_INTEREST))) implies Variability.V_verifyTransferLimits(dt) = true)
```
V11 resolution: Add V11

\[
\text{inv V11:}
\]
\[
\text{processing} -> \forall (dp: \text{Data\_Processing}) |
\]
\[
\text{dp.actors} -> \exists (a | a.\text{type} = \text{Actor\_Type::NON\_PROFIT\_ORGANIZATION}) -> \forall (a |
\]
\[
a.\text{canLodgeComplaints} = \text{true})
\]

V12 resolution: -V12 resolution: Replace C35 by V12, and add V12_2

\[
\text{inv V12_1:}
\]
\[
\text{Corrective\_Action.allInstances()} -> \forall (ca: \text{Corrective\_Action}) |
\]
\[
(ca.\text{type} = \text{SA\_Corrective\_Action\_Type::ADMINISTRATIVE\_FINES} \land (ca.\text{main\_intervenant}.\text{obligation} ->
\]
\[
\text{exists}(\text{obligation: Obligation | not obligation.isFulfilled}) \lor ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::CHILD\_CONSENT\_VIOLATION}) \lor ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::OBLIGATION\_VIOLATION}) \lor ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::CERTIFICATION\_OBLIGATION\_VIOLATION}) \lor ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::CODE\_OF\_CONDUCTS\_MISS\_APPLICATION})) -> \forall (mi |
\]
\[
mi.\text{type} < \text{Actor\_Type::PUBLIC\_ORGANIZATION} \implies ca.\text{TotalFines} = 0.02 *
\]
\[
mi.\text{annualRevenue} \lor ca.\text{TotalFines} <= 10000000
\]
\]
\[
) \land (ca.\text{type} = \text{SA\_Corrective\_Action\_Type::ADMINISTRATIVE\_FINES} \land (ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::PRINCIPLE\_VIOLATION}) \lor ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::DS\_RIGHT\_VIOLATION}) \lor ca.\text{infringement}.\text{type} ->
\]
\[
\text{exists}(\text{Infringement\_Type::CROSS\_BORDER\_TRANSFER\_VIOLATION}) \lor
\]
\[
ca.\text{main\_intervenant}.\text{additional\_obligations} -> \exists (ob | not ob.isFulfilled) \lor
\]
\[
ca.\text{infringement}.\text{type} -> \exists (\text{Infringement\_Type::OTHER\_LOCAL\_LAW\_VIOLATION})) -> \forall (mi |
\]
\[
mi.\text{type} < \text{Actor\_Type::PUBLIC\_ORGANIZATION} \implies ca.\text{TotalFines} = 0.04 *
\]
\[
mi.\text{annualRevenue} \lor
\]
\[
ca.\text{TotalFines} <= 20000000)
\]
\]

V13 resolution: Add V13

\[
\text{inv V13:}
\]
\[
\text{Corrective\_Action.allInstances()} -> \forall (ca: \text{Corrective\_Action}) |
\]
\[
ca -> \forall (\text{Variability.V_setInfrimegementsPenalties(ca)})
\]

V14 resolution: Add 14

\[
\text{inv V14:}
\]
\[
\text{processing} -> \forall (dp | dp.\text{purposes} -> \forall (p |}
\]
\[
\text{Bag { }
\]
\[
\text{Processing\_Context::PUBLIC\_INTEREST, }
\]
\[
\text{Processing\_Context::PUBLIC\_HEALTH}
\]
\[
}) -> \exists (p.\text{context} \implies dp.\text{data\_protection\_impact\_assessment} ->
\]
\[
\forall (dpia | dpia.\text{Consultation} <> \text{ocIIsUndefined()})
\]
\]

V15 resolution: Add V15, implement V_checkedIDProcessing and add the IDENTIFICATION literal to the Data\_Category enumeration

\[
\text{inv V15:}
\]
\[
\text{processing} -> \forall (dp | dp.\text{personal\_data} -> \forall (pd |}
\]
\[
pd.\text{category} = \text{Data\_Category::IDENTIFICATION} \implies \text{Variability.V\_checkIDProcessing(dp) = true}
\]
\]


**V16 resolution:** Add the `EMPLOYMENT_ASSESSMENT` literal to the `DPIA_Information_Type` enumeration

```plaintext
inv V16:
  processing->forAll(dp |
    dp.purposes->forAll(p |
      p._context = Processing_Context::EMPLOYMENT implies dp.data_protection_impact_assessment.
      dpia_information->collect(type)->includes(DPIA_Information_Type::EMPLOYMENT_ASSESSMENT)
    )
  )
```

**V17 resolution:** Add V17, and implement `V_checkDerrogationsFromRights`.

```plaintext
inv V17:
  processing->forAll(dp |
    dp.purposes->forAll(p |
      Bag { Bag { Processing_Context::RESEARCH, Processing_Context::STATISTICAL_PURPOSES 
        } -> includes(p._context) implies Variability.V_checkDerrogationsFromRights(dp) = true 
    } 
  )
```

**V18 resolution:** Add V18, and implement `V_checkDerrogationsFromRights`.

```plaintext
inv V18:
  processing->forAll(dp |
    dp.purposes->forAll(p |
      Bag { Bag { Processing_Context::PUBLIC_INTEREST, Processing_Context::ARCHIVING_PURPOSES }->includes(p._context) 
        } implies Variability.V_checkDerrogationsFromRights(dp)=true 
    )
  )
```

**V19 resolution:** Add V19, and implement `V_checkDerrogationsFromRights`.

```plaintext
inv V19:
  processing->forAll(dp |
    dp.personal_data -> exists(pd | dp.isCoveredByObligationOfSecrecy(pd)) implies 
      Variability.V_checkSARules(dp) 
  )
```

**V20 resolution:** Add V20, and the `CHURCH_OR_RELIGIOUS_ORGANIZATION` literal to the `Actor_Type` enumeration

```plaintext
inv V20:
  processing->forAll(dp |
    dp.actors->exists(type=Actor_Type::CHURCH_OR_RELIGIOUS_ORGANIZATION) implies 
      Variability.V_checkReligiousRules(dp) 
  )
```