BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Volumul 67 (71), Numărul 4, 2021
Secţia
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ
DOI:10.2478/bipie-2021-0019

GDPR RECORDS OF PROCESSING ACTIVITIES FOR DATA CONTROLLERS

BY

CĂTĂLIN MIRONEANU* and CRISTIAN AFLORI

“Gheorghe Asachi” Technical University of Iași,
Faculty of Automatic Control and Computer Science

Received: December 10, 2021
Accepted for publication: December 28, 2021

Abstract. Data controller organizations are required to keep an up-to-date and detailed list of their processing activities and be prepared to show that list to regulators upon request. This list should include at least the purposes of the processing, the target data and all the parties involved in handling that data. We present a solution for organizing all these information into both relational and non-relational document-oriented databases to facilitate such reports. A technical approach of auditing the implementation degree of the rules introduced by the EU GDPR will better prepare the data controllers in complying to this Regulation. We consider a top-down methodology for processing raw data addressing several types of organizations, with different organizational structures. For all these entities we focus on processes, activities, classes of documents collected and personal data. All these data constitute the basis of the “Records of processing activities” required by the Regulation.

Keywords: GDPR compliance; data protection; business analysis; audit; data modelling.

*Corresponding author; *e-mail*: catalin.mironeanu@academic.tuiasi.ro

1. Introduction

Fundamentally, every aspect of our lives revolves around data. Common data processed by an organization include, inevitably, personal data as any information relating to an identified or identifiable natural person. The right to privacy and the right to the protection of personal data have become two one of the most important fundamental rights of modern society. The purpose of the Regulation is to protect all EU citizens against data and confidentiality breaches, and simplify the business environment, so that the citizens and organizations of the European Union can fully benefit from the digital environment.

The EU GDPR clarifies that the responsibility for the protection of privacy lies with any organization operating under the conditions described above, if it collects, stores, manages, and analyses personal data. In this context, there are the three core elements around which all GDPR principles are interpreted: the data controller, the data subject, and the processor. Organizations that have at least 250 employees or conduct higher-risk data processing are required to keep an up-to-date and detailed list of their processing activities. If these organizations determine the purposes and means of the processing of personal data, then they are controllers and must be prepared to show that list to regulators upon request.

Published for the first time in 2016, the "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*" (GDPR or Regulation) was enforced into effect on May 25th, 2018. Despite its importance and implications, there are only a few attempts to try a technical approach to solving the problems raised by the newly introduced rules and their respective correlations. One notable and truly technical approach was made by French "Commission Nationale de l'Informatique et des Libertés", with the open-source PIA (Privacy Impact Assessment) software that helps processors to carry out data protection impact assessment. This is in itself another particularly important topic of interest, and it is complementary to our approach.

Another attempt assumes the premise that GDPR implementation must be from an Enterprise Resource Planning (ERP) perspective. Such a perspective could induce a lot of flat data, thus favoring a structured approach. This data is linked to suppliers, customers, or various kinds of processing purposes, without considering the relationship between the Regulation rules and the personal data processed by an organization.

There are also some software solutions that particularly address article 30 of GDPR and solve only one part of the problem, without taking into consideration the whole links with organizational structures or data categories processed in different data flows.

Consequently, we consider that a strong analysis should begin with operational procedures, personal data flows and the hierarchical structure that defines an organization. Such an approach would be more appropriate in complying with the Regulation principles and would move the focus on the protected assets – personal data.

2. Conceptual Similarities Between GDPR and Other Standards

Implementing GDPR in an organization is much easier if that organization already has passed other standardization processes related to quality management and information security.

ISO 9001:2015 is a mandatory step for all organizations that want to comply with the GDPR requirements. The key benefits related to GDPR are addressing risks and opportunities associated with its context and objectives, and the ability to demonstrate conformity to specified quality management system requirements. The implementation of this standard brings conformation with quality management principles such as process approach, relationship management or evidence-based decision making, to name just a few. One key remark is that compliance with this standard is only a first necessary step in fully following the GDPR requirements. A short but useful analysis of GDPR implementations based on ISO 9001:2015 standard was provided by (Tzolov, 2018). Following the author's conclusions, we deduce the ISO 9001:2015 specifications can be used as a methodology in addressing the Regulation, but it is not sufficient only by itself. Tzolov also enumerates ISO/IEC 27017 and ISO/IEC 27018 standards, which are focused on security techniques. It is a good point of view, but such security concerns are not presently addressed in our paper.

ISO/IEC 27002:2013 is used as a reference for determining and implementing controls for information security risk control in an information security management system (ISMS) based on ISO/IEC 27001. ISO/IEC 27002:2013 deals with the information security in terms of the security of an entity (person, system, organization) defined as a set of measures and means to ensure all conditions so that entity could achieve the objectives for which it was created. From a technical point of view on this standard, information security refers to the protection of information and information systems, unauthorized access, use, disclosure, interruption, modification, or destruction. This results in the security attributes of the information: confidentiality, integrity, availability, authenticity, and non-repudiation.

Regulation recital 90 highlights several PIA elements that overlap with the well-defined risk management components described in clause 6 of ISO 31000:2018. This clause defines processes like establishing scope, context or criteria, risk assessment, risk treatment, communication & consultation, recording & reporting or monitoring & reviewing. The corresponding Regulation

article 24(1) stipulates that technical and organizational measures shall be reviewed and updated where necessary.

Summarizing the previous paragraphs, we conclude that personal data protection must be performed after implementing the corresponding security measures in any organization, including the risk assessment process.

NIST 800-53 standard clearly defines the relationship between requirements and controls. The term *requirements* is strictly defined as information security and privacy obligations imposed on organizations and, in a broader sense, to refer to an expression of stakeholder protection needs for a particular system or organization. *Controls* are defined as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. NIST 800-53 hierarchical control structure is a relevant example of implementing relationship between the GDPR terms in this paper.

3. Database Design Key Concepts

The analysis we performed for the design phase of our solution involved hierarchical, network and relational database design principles. We have determined that relational design patterns could be implemented using document-oriented JSON schemas (Harrison, 2015). The adoption of non-relational patterns was not driven by the limitations of ER modelling (Hills, 2016). We focused on achieving a generic solution that could be easily adapted to various GDPR records of processing activities. In this section we will provide arguments and solutions that are beyond the database model that will be used, providing both relational design and/or document-oriented approaches.

We have identified three types of input data:

1. *GDPR related data*: categories of data subjects, personal data categories, personal data included in these categories, the purposes of the processing, the legal basis of the processing, etc.;

2. *Organizational structure and business processes related to specific activities* – according to quality management implemented standard and GDPR key term of accountability (Sharma, 2020). Implementing the 2nd principle relating to processing of personal data, in compliance to Regulation article 5.2, also involves knowledge on the person nominated by the organization for any activity that involves processing the personal data of the subjects;

3. *The mapping of previous data input* – which is also organizationally specific, but at the highest degree of granularity, according to internal procedures. To further emphasize this requirement, let us consider the data available on an ID card. The person's name and date of birth fall into the identification and personal characteristics category. The unique national identification number is included in the ID-like data category of the data processor, while the address and other supplied information are personal data (Morin, 2016; Taal and Fadahunsi, 2021).

There are two types of output data:

1. *Records of processing activities* – which is the main result and the purpose of collecting all the data required for the documents related to Regulation article 30;

2. *Various control metadata* that could be used to identify which personal data categories and values had been used, what process(s) and activities had been applied to that data, who performed the actual data processing according to Regulation articles 4(2), 5 and 24; this output also yields information for NIST 800-53 *Controls* and could be used to check whether such *controls* have been passed/satisfied. It could be valuable for any personal data internal audit activity or regulators upon request.

We modeled the data layer for the identified input and output using five types of entities that are described in the following subsections.

3.1. Nomenclature Entities

These are the simplest entities, having a key-value structure. It is the natural layout for any document-oriented JSON based data structure. They could also be easily implemented using a relational approach with an id field and a value/description one.

The main purpose of this kind of entities is to allow us to model the information for the *knowledge-based entities*.

3.2. Knowledge-Based Entities

These are core, pivotal entities that we use to model processes, activities, procedures and so on. Almost all the other entities depend on this category (Coronel *et al*., 2020). For example, the organizational structure is mapped using such an entity. In a relational approach, this kind of entity involves a recursive relationship for implementing a hierarchical organizational scheme in a tree-like data structure. Similarly, processes might include sub-processes (*i.e*., university admission process has EU, EEA countries students' admission and non-EU students' admission subprocesses). We are able to model both linear and composed processes using only this single type of entities. The main particularity of the *process* entity is that it contains multiple tree structures; the root for every such tree is modeled by a NULL ID for the parent process.

The hierarchical tree-like structure of these knowledge-based entities is highly flexible. For instance, we can model multiple data controllers, each having its own hierarchical structures and sub-structures. There is a one-to-one mapping between the *organization* entity and the *organizational structure* one. The latter is following the previously mentioned tree-structure and we have enriched the meaning of the ID field:

– a NULL value means that we are dealing with the parent/root structure of the hierarchy;

– a positive integral value symbolizes the ID of the parent structure for the current subordinate;

– a negative integral value means that we are dealing the parent/root structure, but the "data protection officer" (DPO) duties are handled by another external party (company or authorized person).

Another *knowledge-based entity* that is of interest is the *activity* entity. A leaf node subprocess or a linear process can have multiple activities. Keep in mind that processes are not collectors of documents, but related activities are and it is these documents that contain personal data. Using our proposed approach, a PIA analysis would flow naturally from *activity* entities to their corresponding container *process* and therefore allow PIA per process.

3.3. Transactional Entities

The so called *transactional* or *fact* entities are specific only to relational design. The term "transaction fact table" was coined from dimensional data model described in (Kimball, 2013). These types of entities are generated through applying normalization steps in many-to-many relationships. They describe all kinds of combinations make use of data. We use these entities to handle the particular 3rd case of input data previously described. For example, in conforming to the 1st principle of personal data processing stated by GDPR article 5(1(a)), it is need to allow multiple combinations between two nomenclature entities: *laws* and *purposes* of data processing. A particular *purpose* may have multiple *laws* involved, that can be dynamically changed and one single *law* may cover multiple *purposes* of data processing. Of course, the simple case of one-to-one mappings between *laws* and *purposes* is easily covered in such a design.

3.4. Volatile Entities

We have included in this category all the nomenclator entities (Coronel and Morris, 2018) that have a dual interpretation in the Regulation context.

Regulation article 4(7) specifies that data controllers determine the purposes and means of the processing of personal data. Regulation article 4(8) specifies that the processor handles personal data on behalf of the controller. Regulation article 4(1) specifies that a data subject is an identified or identifiable natural person and Regulation applies to the processing of personal data of data subjects. Considering the particular example of "Gheorghe Asachi" Technical University of Iaşi or any University, a classic example of data processor is a bank that processes personal data of students for scholarships and University's employees for salaries. Both students and employees are data subjects for the processor (Vrabec, 2021). On the other hand, some University's employees are

responsible for processes that are handling personal data of the students. From this point of view, University's employees are not data subjects, neither is the controller because there is one data controller – the University.

Another entry in the implementation of a pivoting entity is a volatile nature of a data subject. All applicants to a university would be data subjects and would provide the same personal data for the admission *process*. One of the *activities* included in the admission *process* involves the university presenting the results of the admission contest. Applicants that pass the contest are involved in the next *activities* (for instance: the faculty enrollment *activity*, exam *activities*, scholarship contest *activities*, and so on), while applicants that fail are not. For the latter group, the data processor (*i.e.*, the university) must stop working on their personal data in its next activities. The obvious exceptions are the law-enforced archiving *activities*.

3.5. Records of Processing Activities Entities

These entities are specific to this proposal. Design concepts used in this proposal allow each personal data controller to ad-hoc prepare a *record of processing activities* under its responsibility and provide it to the supervisor authority on request, in respect to Regulation article 30(4). Physical implementing of all previous 4 types of entities allows just one SQL statement that query all necessary tables to obtain the result in a relational database or a complex aggregate operation in a NoSQL database to obtain the same result. We have designed this category of entities to comply with Regulation article 30(3) that stipulates that such records shall be in writing, including in electronic form. The traceability forms of all-time versions of Regulation required *records of processing activities* must be stored in a non-repudiation manner with respect to the security attributes of the information (Huey, 2017). Such entities must be enforced in implementation with secure auditing mechanisms for proving the creation timestamp and no other CRUD operations are further made – with the obvious exception of *Read* (Connolly, 2018).

4. Examples of Implementation Results and Discussions

We have implemented a first variant of the designed solution using a relational database that natively offers support for recursive relationships, using Oracle's "connect by" clause (Ashdown *et al.*, 2018; Helskyaho, 2015). Successful tests were performed on IBM DB2 database using the same "connect by" clause (Molaro, 2013; IBM, 2018; IBM, 2019) and a proof-of-concept test has been performed on a PostgreSQL database using "with recursive" clause (Dombrovskaya *et al.*, 2021; Le and Diaz, 2021).

For the nonrelational variant, we have chosen to use a NoSQL Document-Oriented Database – MongoDB (Sharma, 2021). Successful tests just for proof-

of-concept were also performed on OrientDB database (Tesoriero, 2013). For this latter test category, we have organized the entities into classes. OrientDB uses the concepts of classes and clusters as its form of collections for grouping documents. Throughout the remainder of the article, the term collection is used to represent the implementation of a NoSQL Document-Oriented database.

A total of 33 tables were implemented in the relational database. We only required 12 collections for the NoSQL Document-Oriented JSON. It is worth noting that the number of collections may vary depending on the architectural style adopted.

We used the organizational schema and list of procedures of the Technical University "Gheorghe Asachi" of Iasi as our test data. Alternative tests have been conducted on the data provided by Iasi City Hall.

4.1. Implementation of Personal Data Collected Related Entities

As we mentioned in Section 3, physical or electronic documents contain granular personal data that can be mapped in distinct categories. This means that one category may have multiple personal data types included. Each organization has several types of documents that collect data. Each activity implies documents, and the same document may be involved in different activities. A short test data example: exam registration activity involves a baccalaureate diploma and student enrolment activity involves the same document (please note that in such a case, activities require the same document even if they belong to different processes). This specific document contains the name as personal data from the identity category and high school and grade from the other personal data category.

Table 1 presents samples of input, output, and the corresponding category (referred to as "purpose type") for some of the entities we have discussed in Section 3. We consider this selection to be relevant since it exemplifies the highly relational data required by the *records of processing activities*.

Table 1
Personal data collected related entities types

Entity name	Input data type	Output data type	Purpose type
PersonalDataCategories	GDPR related data	Records of processing activities	Nomenclature
PersonalData	GDPR related data	Control checks	Nomenclature
PersonalDataDocument	Mapping	Control checks	Transactional
CollectedDocTypes	Organizational	Control checks	Nomenclature
ActivitiesCollectedDoc	Mapping	Control checks	Transactional
Activities	Organizational	Control checks	Knowledge-based

The Activities and ActivitiesCollectedDoc are shown in Fig. 1 to better explain an actual case, and there are presented in another example in Subsection 4.2.

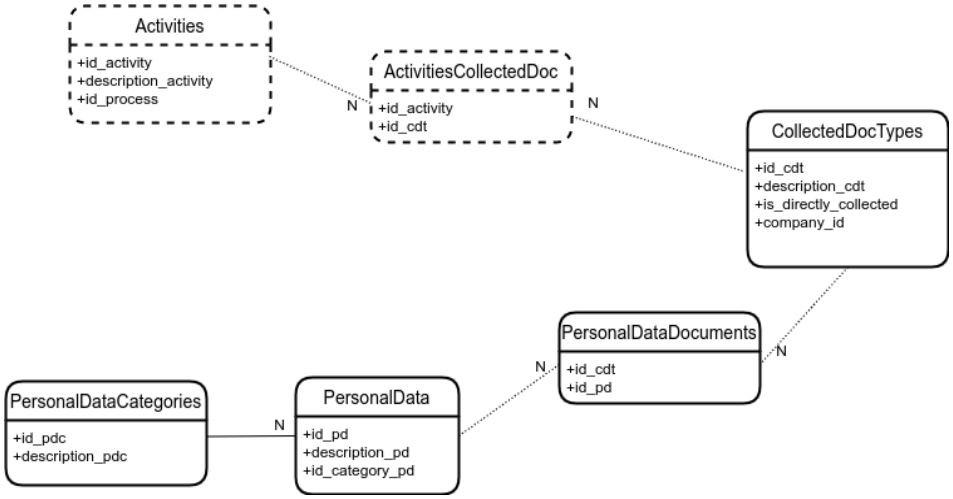

Fig. 1 – Personal data collected related entities.

The corresponding collection for this example is:

```
db.createCollection( "PersonalData",
{
    validator: { $jsonSchema: {
            {
                "bsonType": "object",
                "required": [
                    "description",
                    "category"
                ],
                "properties": {
                    "name": {
                        "bsonType": "string",
                        "description": "required and must be a string"
                    },
                    "category": {
                        "bsonType": "string",
                        "description": "required and must be a string"
                    }
                }
            }
        }
    }
})
```

Fig. 2 – PersonalData collection.

We chose to implement PersonalData collection in this manner because the represented entity is an input type data with respect to GDPR. This kind of data is further used in various documents collected by the data processor. In a

top-down analysis, documents contain personal data, but from an application design perspective, personal data types are assembled to define a document.

Our analysis further indicates that in an activity there are more categories of personal data involved, and an activity implies collecting many types of documents. To normalize such a triad of many-to-many relationship between entities, the quick solution can be a transactional entity linked by the three corresponding IDs. But in a multi-organization environment analysis, such a solution is not suitable because the content of some documents can be different. From this reason, the CollectedDocTypes entity has a company_id attribute. The full ER schema has been normalized through using two transactional entities instead of one. This logical reasoning has also been used is implementing the PersonaDataDocuments collection (Fig. 3).

```
db.createCollection( "PersonalDataDocuments",
{
    validator: { $jsonSchema: {
            {
                "bsonType": "object",
                "required": [
                    "description",
                    "isDirectlyCollected",
                    "refCompany"
                    "personalData"
                ],
                "properties": {
                    "description": {
                        "bsonType": "string",
                        "description": "required and must be a string"
                    },
                    "isDirectlyCollected": {
                        "bsonType": "bool",
                        "description": "required and must be a string"
                    },
                    "refCompany": {
                        "bsonType": "objectId",
                        "description": "reference to the Companies collection"
                    },
                    "personalData": {
                        "bsonType": "array",
                        "minItems": 1,
                        "uniqueItems": true,
                        "items": {
                            "bsonType": "object"
                            "description": "details of the personal data to be collected",
                            "required": [
                                "description",
                                "category"
                            ],
                            "properties": {
                                "description": {
                                    "bsonType": "string",
                                    "description": "required and must be a string"
                                },
                                "category": {
                                    "bsonType": "string",
                                    "description": "required and must be a string"
                                }
                            },
                        },
                        "description": "required and must be an array of personal data subdocuments"
                    }
                }
            }
        }
    }
})
```

Fig. 3 – PersonalDataDocuments collection.

For brevity, we have neglected the previous statements in favor of a better perspective on the PersonalData entity which is more important to achieving the goal of obtaining *records of processing activities*. In Table 1 it can be observed that single *records of processing activities* output data type is for PersonalDataCategories entity and not the PersonalData one, in respect to Regulation article 30(1). Internally, an application like this must focus on the PersonalData entries instead of PersonalDataCategories because it is quite simple to aggregate all categories of personal data collected to assemble a full report.

4.2. Implementation of Activities Related Entities

As we mentioned in Subsection 4.1, each *activity* requires multiple document types and the description of CollectedDocTypes entity was provided in previous explanations. For this reason, this entity and related ActivitiesCollectedDoc and Activities are shown in Fig. 2. Also, these three entities will not be rewritten in Table 2.

Table 2
Activities that involve personal data collection related entities types

Entity name	Input data type	Output data type	Purpose type
Procedures	Organizational	Control checks	Knowledge-based
ProceduresTypes	Organizational	Control checks	Nomenclature
Processes	Organizational	Records of processing activities	Knowledge-based
OrganizationalStructure	Organizational	Control checks	Knowledge-based

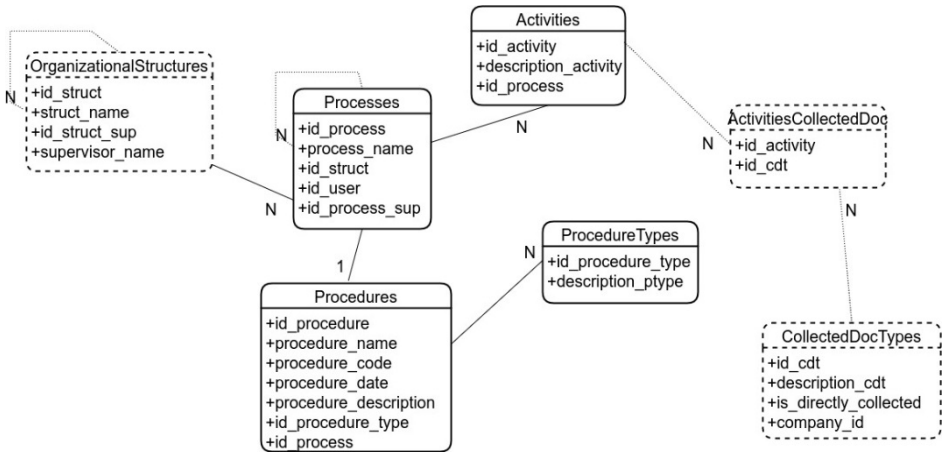

Fig. 4 – Activities that involve personal data collection related entities.

Fig. 4 is also a snapshot of the master ER diagram. The purpose of this short example is to provide the logic of governance. It can be observed in Table 2, in input data type column, that all entities are organizational type. As we briefly stated in the conclusion of Section 1, a proper analysis includes the operational procedures, the personal data flows, the hierarchical structure that defines the organization and the relations between the three data sources.

Each and every node of an organizational structure is governed by processes and related subprocesses, and any process must be regulated by a procedure. Following the example of admission process provided in Section 3, it is important to emphasize the concept of one procedure for a process and many activities in a subprocess. If the process has no subprocesses it is quite simple to link activities to one process. In this case, the procedure is rather simple because there is only one flow of activities.

In this particular example, the relevance of JSON collection structure is a minor one.

4.3. Implementation of Records of Processing Activities Related Entities

We state that Regulation article 30(3) stipulates that such records shall be in writing, including in electronic form. We explained in Section 3 the mechanism to solve this in a non-repudiation manner. In this subsection we will focus on how to obtain the aggregate data and not on how to store the results. The solution of implementing a secure auditing mechanism is dependent on physical implementation, being particular for chosen database. The following Fig. 5 summarizes all the components that are required to assemble the desired *records of processing activities*. As can be noted, the proposed solution offers support for all the needed information. Furthermore, one may expand or decrease the details of the selected data.

The record is a resulting document with auditing and analytical purposes, which must reflect the actual usage of the data controller and the processor of personal data. It allows controllers to precisely identify, among others:

- the actors involved (controller, processors, representative, joint controller, etc.) in the data processing;
- the categories of data processed;
- the purpose of the processing (what previously mentioned actors do with the collected personal data), who has access to and who are the recipients of the personal data;
- for how long is the personal data retained;
- the technical and organizational security measures implemented.

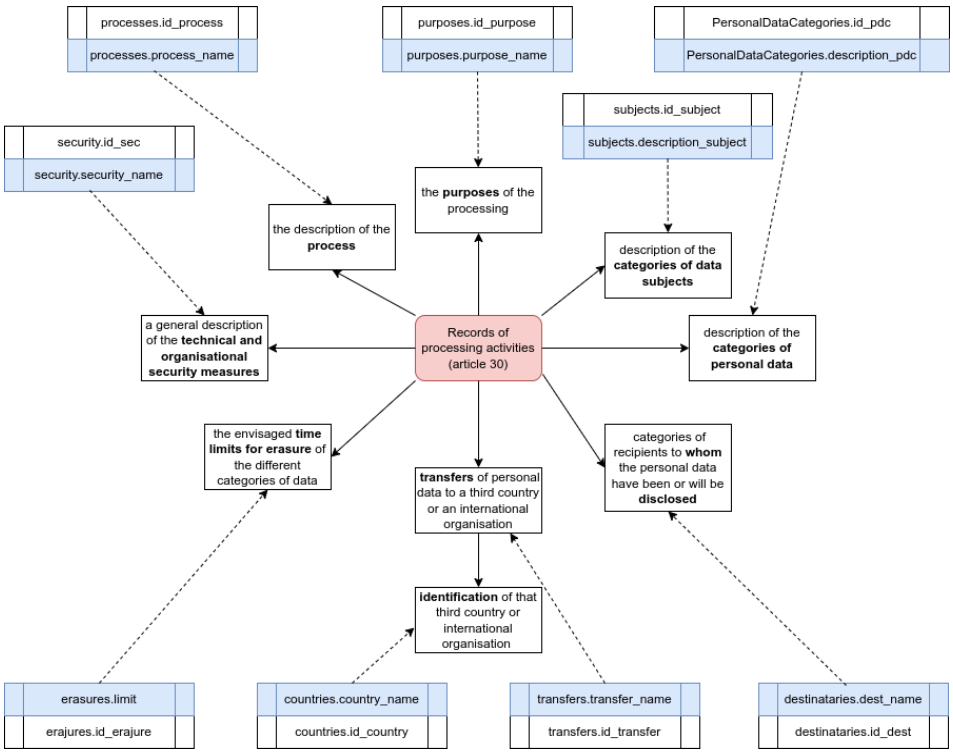

Fig. 5 – Records of processing activities content and related entities.

Regulation article 30(1) stipulates the content of records of processing activities for data controllers, but there is no standard form provided. Reasoning on this particular GDPR article, we concluded that there are 9 columns with meaningful data. All these data are provided by description attributes (in a relational manner) or values (in a NoSQL Document-Oriented manner). Some fields from Figs. 1 and 4 can be seen in Fig. 5, and while there are many examples not shown in this article, we believe they can be deduced based on the explanations provided.

5. Conclusion

The recording obligation is stated by article 30 of the GDPR. It is a tool to help us to be compliant with the Regulation. Aside from being an obligation settled by article 30 of the GDPR, the record is an internal auditing control tool that allows to document data processing activities and to determine the right answers for questions like: Is it really needed to have a specific data set for this processing? Is the data legally collected? Are the data sufficiently protected? Is it relevant to retain all this data for so long?

Another benefit of creating and updating the record are the opportunities to identify and to hierarchize the processing risks considering the GDPR.

We propose in this paper an analysis starting from operational procedures, personal data flows applied on a hierarchical organizational structure, and we consider that this approach is appropriately attuned to the regulation principles.

This paper focuses on business analysis and proper database design in two important types of databases: the relational databases and NoSQL Document-Management ones. Being an analysis proposal, the emphasis fell on fully understanding the Regulation principles correlated with appropriate standards like ISO/IEC or NIST, rather than a comparative performance analysis with the previously mentioned implementations.

Acknowledgements. Both authors have developed business analysis and contribute equally to database design and tested the practical implementation. Cătălin Mironeanu formulated the theoretical and practical models based on standards' analysis and has developed the entity-relationship design and implementation in a relational database. Cristian Aflori validated the theoretical approach and has developed the NoSQL Document-Oriented database design and implementation in a NoSQL database.

REFERENCES

Ashdown L., Keesling D., Kyte T., *Oracle Database Concepts 21c*, Oracle Press, F31733-04, 2021.

Connolly T.M., Begg C.E., *Database Systems: A Practical Approach to Design, Implementation, and Management (6th Edition)*, Pearson Education Limited, 2015.

Coronel C., Morris S., *Database Systems: Design, Implementation, and Management (13th Edition)*, Cengage Learning, 2018.

Coronel C., Morris S., Crockett K., Blewett C., *Database Principles: Fundamentals of Design, Implementation, and Management (3rd Edition)*, Cengage Learning, 2020.

Dombrovskaya H., Novikov B., Bailliekova A., *PostgreSQL Query Optimization*, Apress, 2021.

Harrison G., *Next Generation Databases*, Apress, 2015.

Helskyaho H., *Oracle SQL Developer Data Modeler for Database Design Mastery*, Oracle Press, 2015.

Hills T., *NoSQL and SQL Data Modeling: Bringing Together Data, Semantics, and Software*, Technics Publications, LLC, 2016.

Huey P., *Oracle Database Security Guide 12c Release 1 (12.1)*, Oracle Press, E48135-19, 2017.

IBM, *IBM i 7.4 Database Db2 for i SQL Reference*, 2018.

IBM, *IBM i 7.4 Database Performance and Query Optimization*, 5770-SS1, 2019.

Le Q.H., Diaz M., *Developing Modern Database Applications with PostgreSQL*, Packt Publishing, 2021.

Molaro C., Parekh S., Purcell T., Stuhler J., *DB2 11 The Database for Big Data & Analytics*, MC Press, LLC, 2013.

Morin L., *Oracle Database Development Guide 12c Release 1 (12.1)*, Oracle Press, E41452-07, 2016.

Sharma M., *MongoDB Complete Guide*, BPB Publications, 2021.

Sharma S., *Data Privacy and GDPR Handbook*, John Wiley & Sons, 2020.

Taal A., Fadahunsi O., *The GDPR Challenge: Privacy, Technology, and Compliance in an Age of Accelerating Change*, A Proposal for Multiple Instance Learning Framework Application to Protect Data Access Rights under General Data Protection Regulation (GDPR), CRC Press, 56-66, 2021.

Tesoriero C., *Getting Started with OrientDB*, Packt Publishing, 2013.

Tzolov T., *One Model for Implementation GDPR Based on ISO Standards*, 2018 International Conference on Information Technologies (InfoTech), 1-3.

Vrabec H.U., *Data Subject Rights under the GDPR*, Oxford University Press, 2021.

⁎*⁎ *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, https://eur-lex.europa.eu/eli/reg/2016/679/oj, last visit on October 2021.

⁎*⁎ *ISO 9001:2015 Quality Management Systems – Requirements*, Ed. 5, https://www.iso.org/standard/62085.html, last visit on October 2021.

⁎*⁎ *ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements*, Ed. 2, https://www.iso.org/standard/54534.html, last visit on October 2021.

⁎*⁎ *ISO/IEC 27002:2013 Information Security, Cybersecurity and Privacy Protection – Information Security Controls*, Ed. 2, https://www.iso.org/standard/54533.html, last visit on October 2021.

⁎*⁎ *ISO 31000:2018 Risk Management – Guidelines*, Ed. 2, https://www.iso.org/standard/65694.html, last visit on October 2021.

⁎*⁎ *Kimball Dimensional Modeling Techniques*, Kimbal University http://www.kimballgroup.com/wp-content/uploads/2013/08/2013.09-Kimball-Dimensional-Modeling-Techniques11.pdf, last visit on October 2021.

⁎*⁎ *Manulul procedurilor Universității Tehnice „Gheorghe Asachi" din Iași*, https://www.tuiasi.ro/manualul-procedurilor/, last visit on October 2021.

⁎*⁎ *Organigrama Primăriei Municipiului Iași*, http://www.primaria-iasi.ro/portal-primaria-municipiului-iasi/organigrama-pmi/9617/organigrama-rof-cod-etic, last visit on October 2021.

⁎*⁎ *Organigrama Universității Tehnice „Gheorghe Asachi" din Iași*, https://www.tuiasi.ro/wp-content/uploads/2021/05/organigrama-2021.pdf, last visit on October 2021.

⁎*⁎ *Privacy Impact Assessment*, Commission Nationale de l'Informatique et des Libertés (CNIL), https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment, last visit on October 2021.

[*,*] *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-53, Rev. 5, September 2020, https://doi.org/10.6028/NIST.SP.800-53r5.

EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE PENTRU OPERATORII DE DATE CU CARACTER PERSONAL

(Rezumat)

Organizațiile operatoare de date cu caracter personal trebuie să păstreze o listă actualizată și detaliată a activităților de prelucrare a acestor date și să fie pregătite să prezinte, la cerere, această listă autorităților de reglementare. Lista ar trebui să includă scopurile prelucrării, ce fel de date vor fi prelucrate, cine are acces la ele în cadrul organizației, dar nu numai. În această lucrare se propune o modalitate de organizare a tuturor acestor tipuri de date cu caracter personal, atât într-o manieră relațională, cât și într-un design NoSQL orientat pe documente. O abordare tehnică de auditare a gradului de implementare a normelor introduse de GDPR va pregăti mai bine operatorii de date cu caracter personal pentru obținerea conformității cu acest Regulament. Luăm în considerare o metodologie cu abordare de sus în jos pentru prelucrarea datelor brute, în situații organizaționale multiple, cu structuri organizaționale diferite, continuând cu procese, activități, categorii de documente colectate și finalizând cu datele cu caracter personal. Toate acestea conduc la realizarea Evidenței activităților de prelucrare prevăzute de Regulament.