September 2023

Towards a Semantic Specification for GDPR Data Breach Reporting

Harshvardhan J. PANDIT [a,b,1], Paul RYAN [a,b,e], Georg Philip KROG [d], Martin CRANE [b], Rob BRENNAN [a,c]

[a] *ADAPT SFI Research Centre*
[b] *Dublin City University, Dublin, Ireland*
[c] *University College Dublin, Dublin, Ireland*
[d] *Signatu AS, Oslo, Norway*
[e] *Uniphar PLC, Dublin, Ireland*

ORCiD ID: Harshvardhan J. Pandit https://orcid.org/0000-0002-5068-3714, Paul Ryan https://orcid.org/0000-0003-0770-2737, Martin Crane https://orcid.org/0000-0001-7598-3126, Rob Brennan https://orcid.org/https://orcid.org/0000-0001-8236-362X

Abstract. Data breaches and other security incidents are an emerging challenge in the digital era. The General Data Protection Regulation (GDPR) requires conducting an impact assessment to understand the effects of the breach, and to then notify authorities and affected individuals in certain cases. Communication of this information typically takes place via conventional mediums such as emails and forms on the websites of authorities, and is a manual process. To assist in developing tools to support data breach investigations, and to enable automated systems for assisting with breach assessments and GDPR compliance, we present a machine-readable specification for the representation and documentation of information related to data breaches and their communications. The specification uses current requirements from the GDPR obligations and authoritative guidelines. To represent information, it extends the Data Privacy Vocabulary (DPV) by introducing new concepts required for data breach relevant information.

Keywords. GDPR, data breach, cybersecurity, semantics

1. Introduction

The General Data Protection Regulation (GDPR) requires data breach notifications to be sent to authorities and data subjects based on an assessment of the breach's impact on rights and freedoms. Conducting such assessments is difficult in practice due to lack of knowledge regarding what risks exist and how to associate them with the factual information available regarding a breach. Further, reporting the breach also involves additional information not explicitly required by the GDPR - for example the Irish Data

[1] Corresponding Author: Harshvardhan J. Pandit me@harshp.com. This research was conducted with the financial support of Science Foundation Ireland under Grant Agreement No. 13/RC/2106_P2 at the ADAPT SFI Research Centre at Dublin City University.

Protection Commission's data breach reporting form provides a specific list for 'nature of the breach' which includes events such as 'processing error' and 'unauthorised access to personal data' via different mediums. Other authorities' websites have similar forms that provide a different set of information. With increased cybersecurity reporting requirements through laws such as the Network and Information Security Directive (NIS2, 2023) and Digital Operational Resilience Act (DORA, 2023), the process of reporting security incidents such as data breaches will require more information and communications amongst a larger pool of parties. Relying on conventional documentation and communication measures therefore represents a barrier to effective compliance.

We present a specification to define information regarding data breaches in a machine-readable form (by using semantic web standards such as RDF) so as to address these challenge and enable the development of interoperable tools for assisting organisations and authorities in their data breach requirements. In this, we reuse and extend the Data Privacy Vocabulary (DPV) [1] which enables machine-readable representation of information related to GDPR, and has been used for documenting Register of Processing Activities (ROPA) [2] and Data Protection Impact Assessments (DPIA) [3]. Our contributions provide the necessary concepts to represent information about data breaches, documentation pertaining to reporting of data breaches, and notifications communicated regarding data breaches. The resulting specification[2] is being published by the W3C Data Privacy Vocabularies and Community Group (DPVCG) to provide data breach concepts and guidance as well as in the continued refinement of the risk and impact assessments.

2. Background and State of the Art

GDPR Article 4-12 defines a 'personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." The European Data Protection Board (EDPB), in its Guidelines 9/2022 on personal data breach notification [4] interpret this definition to formulate three categories where personal data is unlawfully or accidentally breached. These categories are: 'Confidentiality breach' for disclosure or access; 'Integrity breach' for alteration; and 'Availability breach' for loss of access or destruction. Thus, a data breach under GDPR spans a broader spectrum of processing activities over personal data than the conventional use of the term which is limited to unauthorised access. Further information on the requirements for handling data breaches are found in GDPR's Articles 33 (notifying authority), 34 (notifying data subject), 39 (DPOs), and 55 (authorities). To assist with these obligations, data protection authorities such as the Irish Data Protection Commission (DPC) have issued guidelines [5] and developed a form on their website for convenient reporting of data breach.

The novelty of data breach obligations under the GDPR has attracted interest from diverse stakeholders. Schlackl et al. [6] have analysed the causes and consequences of data breaches, and found that data breaches are caused by and affect a wide variety of domains, including internal organisational processes. Their analysis provides the necessary background information on how to link a data breach assessment to internal organisational processes, and how to represent the causes and consequences related to a data

[2] `https://w3id.org/dpv/guides/data-breach`

breach. We utilise these as the knowledge for enrichment of DPV's risk assessment concepts, and for use within the data breach reports and impact assessments. The DEFeND H2020 project utilises machine-readable information in its "privacy by design platform for GDPR compliance", which includes modules associated with data breach monitoring and notifications to data subjects [7], but does not provide details regarding the implementation of these features.

Efforts to consolidate knowledge regarding data breaches has led to the creation of a "Global Data Breach Database" [8] which lists the data breaches known to have occurred based on publicly available information. However, the database is rather limited in terms of available information, and its information is also not available in a machine-readable form for automated ingestion and analysis. Several initiatives exist that model security information in a machine-readable form, such as VERIS[3], MISP[4], and MITRE - whose taxonomies such as Common Vulerabilities and Exposures (CVE) [9] are widely utilised to represent security related information. Our specification is complimentary to these as it concerns keeping records and communicating regarding data breach incidents based on regulatory requirements as outlined in GDPR.

3. Data Breach Specification

Based on the requirements of the GDPR and its interpretation within the state of the art as presented in Section 2, we define the following requirements for information to be provided by the specification:

1. Information about the existence of a Data Breach i.e. whether it has occurred, is occurring, or has been mitigated. We term this as information about the 'lifecycle' of the breach – represented in Section 3.1.
2. Information about the Data Breach itself i.e. when and where did it occur, its cause, affected systems, data, and data subjects – represented in Section 3.2.
3. Investigation of the Data Breach i.e. detection report, what has been affected, who has it been notified to and when – represented in Section 3.3.
4. Notifications i.e. communication between entities, e.g. Controller to DPA, specifying information available at that point in time – represented in Section 3.4.
5. Impact Assessment i.e. assessing risks to rights and freedoms of individuals at that point in time – represented in Section 3.5.

3.1. Data Breach Lifecycle

A data breach incident starts when a breach is suspected or detected, and ends with a final report detailing impacts and mitigation measures taken. In addition to these, organisational processes may involve unclear or ambiguous information, for example - where sufficient information is not available to state whether a breach exists, or where a breach is suspected but not yet confirmed. We created the following stages by extending `dpv:Status` as *DataBreachStatus*: `DataBreachSuspected` represents the case where a data breach is suspected and requires discovery and validity of this suspicion to confirm

[3] `https://verisframework.org/`
[4] `https://www.misp-project.org/index.html`

its existence. `DataBreachDetected` represents the case where a data breach has been detected and requires determining whether it has concluded or is ongoing, and to ascertain its cause, nature, and effect (GDPR Article 33). `DataBreachOngoing` represents the case where a data breach is currently in progress and requires identifying measures to stop the breach. `DataBreachHalted` and `DataBreachConcluded` represent cases where a data breach has stopped of its own accord and without any mitigations - with 'halted' indicating a likelihood of being resumed. `DataBreachTerminated` represents the case where a data breach has been stopped through mitigation measures taken in response and where does not have a likelihood of resuming. `DataBreachMitigated` represents the case where potential similar data breaches have been prevented from recurring through the use of mitigation measures.

3.2. Data Breach Event

The data breach '*event*' represents the occurrence of the breach, and for which documentation is required to be maintained in terms of temporal properties i.e. when the breach started and ended - as its duration. This is indicated using the DCMI Metadata Terms[5]. The '*cause*' of a breach is the event which led to the breach taking place. It is represented using the concept `Threat` and is associated with the breach using `causedByThreat` relation. An example of a source of data breach is where an employee left their office computer unattended without locking it. The lack of security in securing office machines is a vulnerability, represented using the concept `Vulnerability` and associated using the relation `hasVulnerability`. Vulnerabilities represent a weakness or limitation that was exploited in order to create the source event which then leads to the data breach. Vulnerabilities are not necessary for a source to realise, for example an accident can occur without a vulnerability. The '*source*' of a breach is the actor or non-actor source that caused the breach to take place through intentional or unintentional means, and regardless of malicious intent or accidents. It is represented by `ThreatSource` and associated using `hasThreatSource`. The '*type*' of a data breach is based on EDPB's categorisations as '*confidentiality*', '*integrity*', and '*availability*' based on the effect of the breach .

3.3. Data Breach Reports

`DataBreachReport` represents documentation of information, with further subclasses to represent different reporting requirements e.g. when breach is detected and is being investigated, and is classified based on reporting requirements under GDPR as - preliminary, ongoing, and concluded. A preliminary investigation report provides details to be reported within 72 hours of the breach being detected, and is followed up by zero or more ongoing investigation reports, and a final conclusion report. In reporting data breaches, authorities specifically ask for the involved Controllers and Processors which are specified using the relations `dpv:hasDataController` and `dpv:hasDataProcessor` respectively. In addition, authorities also ask about 'cross-border' breaches, which is represented using `dpv:hasJurisdiction` and the relevant EU member states.

[5] `https://www.dublincore.org/specifications/dublin-core/dcmi-terms/`

3.4. Data Breach Notifications

DataBreachNotice represents information being communicated between entities, with specific notices defined for information sent to an Authority, a Controller, a Processor, or a Data Subject. Metadata about the notices is represented using DCMI Metadata Terms and Schema.org vocabularies, e.g. `dct:medium`, `dct:format`, `schema:Message` to describe an email being sent. To indicate whether some notifications are being planned, are ongoing, or have been completed - `dpv:ActivityStatus` is to be used.

3.5. Data Breach Impact Assessment

A Data Breach Impact Assessment (DBIA) is similar to a Data Protection Impact Assessment (DPIA) in that it is undertaken to assess the risks and impacts to data subjects, where the DPIA is intended to address a planned process and the DBIA relates to a data breach that has taken place. A DBIA is essential in order to determine whether to notify authorities and data subjects regarding the breach, and to plan the necessary measures to handle the breach. If the DBIA indicates that the breach is likely to result in a risk to the rights and freedoms of individuals - then the authorities have to be notified. If the DBIA indicates a high risk to the rights and freedoms of individuals - then both the authorities and data subjects have to be notified.

A DBIA is based on the information available at a given time. Therefore, it can be undertaken at any stage in the breach handling process - from preliminary where fewer information is known to final where all information is available. to represent a DBIA, the DPV concept `dpv:ImpactAssessment` is extended as `DataBreachImpactAssessment`. DCMI terms are used to represent relevant metadata similar to the breach reports (e.g. temporal, provenance).

A Data Breach Impact Assessment (DBIA) contains three categories of information:

1. Information about the Breach: Type of breach; Nature, sensitivity, and volume of personal data; Special characteristics of the individual; Special characteristics of the data controller; Number of affected individuals.
2. Risk Assessment: risks and impacts to rights and freedoms, risk levels, likelihoods, severity of consequences, and specific risks (e.g. ease of identification).
3. Outcomes: activities to be undertaken based on the assessment

The information about the breach in terms of what data or individuals have been affected is the same as that present in a Data Breach Report, and therefore can be included through a link to the report itself or explicitly added to the assessment in a manner similar to that of the report. Information about the risk assessment includes the specifics of what risks are applicable, the consequences and impacts arising from it, their severity and likelihood, and the impacted stakeholders - including impacts to the rights and freedoms.

Additionally, breach reporting requires information on applicability of specific risks - such as (re-)identification of individuals through breached data. To associate these risks, the existing DPV risk assessment terms are used e.g. wih `dpv:hasRisk` and `dpv:hasImpact`. Where such risks are absent, they are explicitly declared as `dpv:NotApplicable`. To specify the severity and likelihood, we reuse *dpv:hasSeverity* and *dpv:hasLikelihood*. Further information about risk and impact assessment concepts can be seen in the semantic specification for DPIA [3] which also uses DPV and provides the necessary concepts which are required in a DPIA and are the same within a DBIA.

4. Conclusion and Future Directions

In this article, we introduced a semantic specification for representing information about data breaches based on the requirements of the GDPR. The specification provides a machine-readable vocabulary to represent information regarding the data breach event, how it was detected, the consequent analysis of its impact on systems, data, and data subjects, and its communication to other entities. Through these, we hope to enable efficient tools and processes to handle obligations regarding data breaches, and to make communicating about breaches to be in line with existing cybersecurity methods which already use interoperable taxonomies and automated tooling.

The specification is a preliminary work that establishes the framework of information required and requires analysing guidelines and reporting mechanisms by EU data protection authorities to create a common pan-EU data breach reporting framework. Through this, consistent and interoperable tools can be developed to assist stakeholders such as DPOs and authorities in tasks such as information validation, and to provide assistance in impact assessments by creating communal 'knowledge graphs' to identify relevant risks and impacts similar to existing security initiatives such as MITRE and VERIS. Finally, as data breaches are also security incidents, the specification can also be extended for use with other regulatory requirements such as NIS2 and DORA.

References

[1] Pandit HJ, Polleres A, Bos B, Brennan R, Bruegger B, Ekaputra FJ, et al. Creating A Vocabulary for Data Privacy. In: The 18th International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE2019). Rhodes, Greece; 2019. p. 17.

[2] Ryan P, Brennan R, Pandit HJ. DPCat: Specification for an Interoperable and Machine-Readable Data Processing Catalogue Based on GDPR. Information. 2022 May;13(5):244. Available from: https://www.mdpi.com/2078-2489/13/5/244.

[3] Pandit HJ. A Semantic Specification for Data Protection Impact Assessments (DPIA). Towards a Knowledge-Aware AI. 2022:36-50. Available from: https://ebooks.iospress.nl/doi/10.3233/SSW220007.

[4] Guidelines 9/2022 on Personal Data Breach Notification under GDPR — European Data Protection Board;. Available from: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en.

[5] A Practical Guide to Personal Data Breach Notifications under the GDPR — Data Protection Commission;. Available from: https://www.dataprotection.ie/dpc-guidance/breach-notification-practical-guide.

[6] Schlackl F, Link N, Hoehle H. Antecedents and Consequences of Data Breaches: A Systematic Review. Information & Management. 2022 Jun;59(4):103638. Available from: https://www.sciencedirect.com/science/article/pii/S0378720622000507.

[7] Piras L, Al-Obeidallah MG, Praitano A, Tsohou A, Mouratidis H, Gallego-Nicasio Crespo B, et al. DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance. In: Gritzalis S, Weippl ER, Katsikas SK, Anderst-Kotsis G, Tjoa AM, Khalil I, editors. Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science. Cham: Springer International Publishing; 2019. p. 78-93.

[8] Neto NN, Madnick S, Paula AMGD, Borges NM. Developing a Global Data Breach Database and the Challenges Encountered. Journal of Data and Information Quality. 2021 Jan;13(1):3:1-3:33. Available from: https://dl.acm.org/doi/10.1145/3439873.

[9] CVE - Common Vulnerabilities and Exposures;. Available from: https://cve.mitre.org/.