Digitalising the General Data Protection Regulation with Dynamic Condition Response Graphs*

Emil Heuck[1], Thomas T. Hildebrandt[1], Rasmus Kiærulff Lerche[2], Morten Marquard[2], Håkon Normann[1], Rasmus Iven Strømsted[1], and Barbara Weber[3]

[1] IT University of Copenhagen, 2300 Copenhagen S, Denmark,
eheu,hilde,hnor,rivs@itu.dk
[2] Exformatics A/S, Dag Hammerskjolds Alle 13, Copenhagen, Denmark Ø
mmq,rkl@exformatics.com
[3] Technical University of Denmark, DTU Compute, Asmussens Alle, Building 322, DK-2800 Kgs. Lyngby, Denmark
bweb@dtu.dk

Abstract. We describe how the declarative Dynamic Condition Response (DCR) Graphs proces notation can be used to digitalise the General Data Protection Regulation (GDPR) and make a first evaluation to what extend the formalisation and associated tool for end-user modelling and simulation can be used to clarify the meaning of the GDPR and its consequences for the main business process of a Danish funding agency.

Keywords: GDPR, Formalisation, DCR Graphs

1 Introduction

The digitalisation and use of personal data in organisations have increased and is an integral part of almost any businesses or public organisation. The legislation on the use of personal data, the Data Protection Directive (DPD) from 1995, has been superseded in 2016 by the General Data Protection Regulation (GDPR) [2]. This new law affects all areas of organisations using personal data in some form. The regulation reinforces many of the laws from the DPD in addition to introduce new laws. A change from the former directive is the increase in the fines and the rights of the data subject. As the regulation is set to be enforceable from the 25th of May, 2018, the organisations have less than a year to be compliant. This has many organisation scrambling to understand the new regulation and get in compliance. However, there are still many questions and concerns

* M. Brambilla, T. Hildebrandt (Eds.): BPMN 2017 Industrial Track Proceedings, CEUR-WS.org, 2017. The paper is based on a mini-project supported by the innovation network Infinit.dk

regarding its enactment in practice. What parts of the GDPR will overrule existing laws ? How do organisations ensure that they are in compliance when it comes to ambiguous parts of the regulation? How will the regulation change existing business processes ? In the present paper we describe the results of a proof-of-concept project aiming at testing the idea that these questions could be approached by formalising the GDPR using Dynamic Condition Response (DCR) Graphs [3, 4] and the associated DCRGraphs.net tool supporting end-user modelling and simulation. developed as a collaboration between researchers at the IT-university of Copenhagen and the danish company Exformatics. We evaluated the idea by presenting the formalised GDPR constraints to a GDPR consultant and by merging in the GDPR formalisation with a formalisation of a business process at a funding agency using DCR Graphs as basis for their case management system [1]. The merged processes were then simulated jointly with a case worker.

2 Dynamic Condition Response Graphs

Below we briefly recap the definition of Dynamic Condition Response (DCR) Graphs and the support for modelling and simulation using DCRGraphs.net.

As any other business process notation, the DCR Graphs notation allows for the modelling af business activities/events and the roles af actors who can carry out the activities. The key difference between DCR graphs and e.g. BPMN diagrams is that one does not model the explicit sequence flow between activities. In Figure 1 is shown a DCR graph in the DCRGraphs.net tool modelling the activities and roles for an on-boarding process. The six activities are: GDPR Consent, Sign Contract, First day at work, Need for PC, Order PC, Receive PC. Each activity is assigned a role, e.g GDPR Consent is assigned the role Employee, meaning that only the employee can give the GDPR consent. The formalism allows that an activity can have any number of roles assigned, i.e. an activity without role reflects that the role is still unknown or unassigned, while an activity with more than one role denotes that different roles are allowed to carry out the activity.

The graph in Figure 1 has no constraints between activities, meaning that any activity can be carried out any time and any number of times. This means that any sequence of the activities is possible. If we want to constrain the ordering, we use the DCR graph relations between the activities. Figure 2 illustrates all the possible relations between activities in DCR graphs. The arrow with the bullet at the source, as the one highlighted in the figure from Need for PC to Order PC is the *response* relation, denoting that if Need for PC is carried out (meaning that the HR department registers that the new employee needs a PC, then the activity Order PC must eventually be carried out. As shown in the panel to the right in the figure, it is possible to add guards (making the response conditional on data), time deadlines, a level (making it possible to filter out relations when viewing a complex graph) and a description to the relation. The arrow with the bullet at the target, as the one from GDPR Consent to Sign Contract is

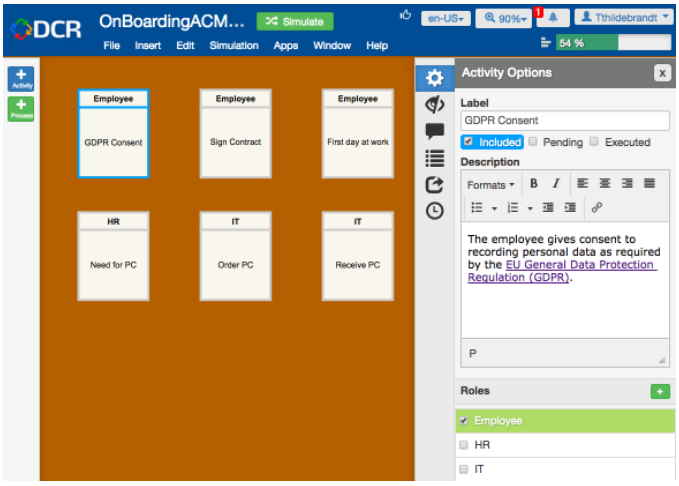

Fig. 1. DCR graph in DCRGraphs.net with six activities assigned roles, but no other constraints.

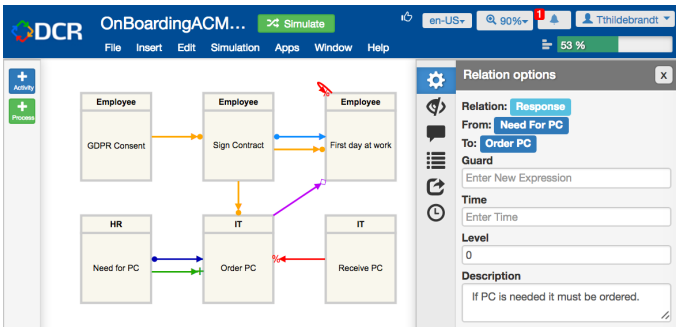

Fig. 2. DCR Graph with relations constraining the sequencing of activities.

the *condition* relation, denoting that GDPR Consent must be carried out before Sign Contract can be carried out. Similarly, condition relations constrain that Sign Contract must be carried out before Order PC and First day at work can be carried out. The arrow with the % sign at the target, as shown from Receive PC to Order PC and from First day at work to itself is the *exclude* relation. This relation denotes that if Receive PC happens, then Order PC is excluded from the graph and thus no longer relevant. The relation with the + sign at the target, as shown from Need for PC to Order PC means that Order PC is included in the graph and thus again relevant. This means that in this process, Order PC can happen any number of times until Receive PC happens, then it is required that Need for PC happens before Order PC can (and because of the response relation must) happen again. The exclude relation from First day at work to itself thus means that this activity can only happen once, since it can not be included

again. Finally, the relation with the rombe at the end from Order PC to First day at work is the *milestone* relation, which means that as long as Order PC is required to happen (because of the response from Need for PC), First day at work can not happen.

The DCRgraphs.net tool allows for collaborative simulation of processes by hitting the green Simulate button at the top. During the simulation the state of the process is shown as a marking of the graph and a traditional swimlane diagram is dynamically showing the sequence activities that has happened during the simulation. The marking of the graph indicates with a green checkmark on an activity that it has happened at least once and a red exclamation mark that it is required to happen (e.g. required as a response) at least once more, unless it is excluded by another activity. Excluded activities is visualised with a dashed border.

3 The General Data Protection Regulation

In this section we briefly introduce the General Data Protection Regulation (GDPR) and show how key paragraphs are formalised as DCR Graphs.

Laws and policies have been implemented to protect this data and specifically personal data. In 1995, the European Parliament enacted into law a *Data Protection Directive* with the intent of securing personal data. The directive has been updated into what is now known as the General Data Protection Regulation (GDPR) in 2016 with the regulation going into application on the 25th of May 2018. [2] Both Public and private enterprises are facing severe challenges as to be in compliance with the new general data protection regulation. The difference from the old directive to this new regulation is that the regulation acts without the need for the implementation of national legislation. As it is with many new regulations and laws, there are many different interpretations of it and how certain aspects of the laws should be viewed. In this paper, we have used the interpretation as seen by the ICO which is an independent public body in Great Britain whose goal is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals". ICO is a public body under the Crown in Great Britain and have been handling data protection laws in the UK since 1984. This regulation's intent is to ensure the protection of the personal data, of the citizens in the European Union. Ultimately, this can be ensured by fining companies, both public and private, with up to 4% of the worldwide turnover if they are not in compliance with the regulation. In this new version of the GDPR, it is not only companies within the EU that needs to be in compliance but also companies outside the EU that processes data from European citizens. This is one of the bigger changes to the regulation as the data protection directive did not include this. The term personal data is defined by the EU as:

> ... personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything

> from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address

This definition is relevant for the thesis as the term personal data differs from data in general and what we are investigating is the usage of personal data by organisations and the newly implemented regulation of this.

Organisations are now expected to implement procedures that help facilitate *privacy by design*. Such procedures include the training of personnel in data security, reviews of policies, transparency, and internal audits, only to mention a few.

> The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

Data Protection Officer (DPO) is a new position implemented in the companies as the GDPR requires certain companies to appoint a Data Protection Officer (DPO) to ensure compliance within the company. These officers should inform the organisation on the GDPR and maintain compliance internally. Furthermore, the officer is the point of contact for the supervisory authority and the individuals whose data is being processed.

Data breaches can happen if the company is negligent or by a malicious outside source hacking into their database. These breaches has to be reported to a specified authority within 72 hours and to the individual if the breach is severe enough. The GDPR is lenient in the amount of information that has to be supplied as the breaches cannot be investigated fully within the 72 hour period. The report can therefore be supplied in stages as more information is uncovered.

Handling of personal data is of course the key issue of the GDPR. The GDPR touches upon several rights of the individual as to how their data is being handled, what data is being used, what access they have to the data and what right they have over their personal data. The GDPR further strengthens the individual's rights of their personal data by allowing citizens to request deletion, anonymisation, rectification of their data. Furthermore, the data subject (the citizen) have to be informed of how and to what end their data is being used and to give their consent to this. This consent can be withdrawn by the subject at any time, requiring the company to default on their data. The citizen also has a right to deletion which has been called *The right to be forgotten*. This right and other rights of the individuals are elaborated upon later.

We decided to make a distinction between the parts of GDPR which is about organisational compliance and process-oriented compliance. The deviation separates into two focus points: establishment of a process, and a process is in use. This distinction is necessary as to what exactly is to be modelled.

Table 1. Key GDPR terms

Term	Explanation
Consent	The freely given acceptance from a data subject that an organisation use their personal data.
Data protection officer	An expert on data privacy who ensures GDPR compliance.
Data subject	A natural person whose personal data is used in an organisation.
Natural Person	A person.
Personal data	Information that identify a data subject
Privacy by design	The concept that privacy is built-in the systems used by organisations.
Regulation	legislative act that must be implemented across the European Union.
Data processing	Any operation performed on personal data.

The process model template focus on process-orientated GDPR compliance. A process model template which contains the aspects of GDPR: Data Handling & Processing, Inquiry of Data and Data Breach, can be added as supporting process model to already existing process models. A supporting GDPR process for processes in use, must therefore be designed in such a fashion that it is compliance with the entire regulation, and model the lawful activity so that it can be implemented at organisations already using DCR. Though organisational compliance does not describe activities for a process model, it has important elements of which describes a behavior of the process. The part of GDPR which applies to when the process is in use is principles, accountability & governance, and privacy by design. It is further important to mention that according to ICO the part of GDPR used for set-up of the process should still be in state where it is always under continuous improvement (ICO.org.uk).

We chose to structure of the GDPR support process using seven broad terms: The Process Instance, Inquiry of New Personal Data, Requests from Data Subjects, Verification, Data Handling, Data Breach Handling, and Documentation. The process Instance is the process to which the GDPR process is a support process. Each Process Instance is a run-time process of with processing of personal data. Therefore the Process Instance is not a part of the GDPR process in itself, but included into the process model in order to understand the relation between the process and the GDPR support process. This is also the case when looking at Verification, as Verification is dependent on how the organisation works, and how the organisation is structured. Yet for Verification, it is requirement (explanation is given in the next section on fragments) to be able to verify if a natural person is the data subject of the process instance, and therefore also part of the GDPR support process.

3.1 Key GDPR paragraphs as DCR Graphs fragments

A key point of using a declarative notation as DCR graphs is that the legal constraints, in this case the GDPR, can be formalised in the same notation

as the business process, but the two formalisations can be made and verified independently of each other. Below in Table 2 we show the key fragments we formalised as DCR graphs.

Table 2. Key GDPR fragments

Give Consent	Verify identity
Inform third parties of rectification request	Restrict processing
Objection	Withdraw consent
Provide confirmation on processing of their data	Inform data subject of third-parties
Lift restriction	Report data breach to authority within 72 hours
Give information on data use	Provide access to their personal data
Delete personal data on data subject	Transfer personal data
Report data breach to data subject with information	Give information about rights
Rectify personal data	Refuse deletion of data
Information about rights	

We have used the ICO.org.uk interpretation of the articles as our basis for the formalisation. Below we give examples of some of these interpretations.

Consent

> Consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes. Individuals have a right to withdraw consent at any time. (ICO.org.uk)

Reference in GDPR: Articles 4(11), 6(1)(a), 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 51, 59, 171 (GDPR, 2017) The formalisation in DCRGraphs.net is shown in Figure. 3.1.

Give information about rights

> The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data. (ICO.org.uk)

Reference in GDPR: Articles 12(1), 12(5), 12(7), 13 and 14 and Recitals 58-62 (GDPR, 2017)

Rectification

> Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate. (ICO.org.uk)

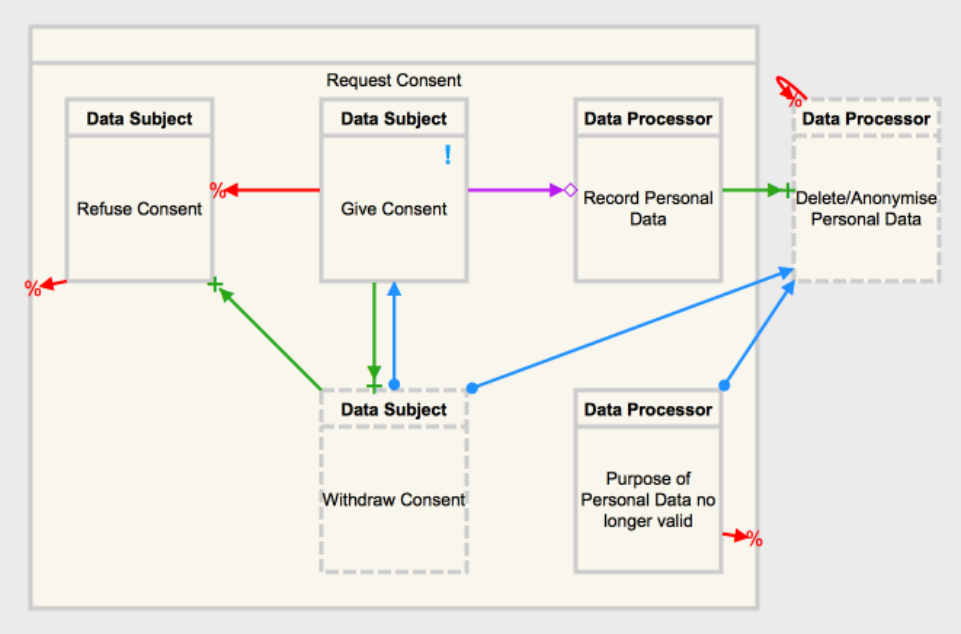

Fig. 3. DCR graph showing the formalisation of the requirements in the GDPR regarding giving and withdrawing consent, independently of a particular business process.

Reference in GDPR: Articles 12, 16 and 19 (GDPR, 2017)

We only give example of one of the formalisations, namely the formalisation of the requirements regarding consents, which can be seen in Figure 3.1. The DCR graph uses a *nesting* activity, Request Consent, which contain five activities Give Consent, Refuse Consent, Record Personal Data, Withdraw Consent and Purpose of Personal Data no longer valid. Give Consent is a pending response (the consent is requested from the Data Subject) and the milestone relation to Record Personal Data is disabling the recording as long as Give Consent is pending. Refuse Consent has an exclude relation to the nesting activity Request Consent, which means that the nesting activity and all activities inside are excluded. When Give Consent happens, it is no longer pending, which means that Record Personal Data becomes enabled. Also, the activity Refuse Consent is disabled, but Withdraw Consent is included, since it is now relevant for the Data Subject to withdraw consent. If Withdraw Consent happens then Give Consent and Delete/Anonymise Personal Data become required (due to the response relations) and Refuse Consent becomes included again. Note that Delete/Anonymise Personal Data is only included if some data was actually recorded. Finally, the deletion may also be required because the purpose seized to be valid, as indicated by the activity Purpose of Personal Data no longer valid which also has a response relation to Delete/Anonymise Personal Data.

4 Evaluation

We now describe the key feedback resulting from our presentations of the GDPR formalisation to a GDPR consultant and a case worker at a funding agency.

4.1 GDPR consultant

The GDPR formalisation was evaluated independently of the Dreyer business case by presenting the formalisation to a consultant trained in DCR graphs, who works professionally helping companies getting compliant with the GDPR. His main comments were that the formalisation was indeed helpful to make the interpretation of GDPR precise, but also that the DCR graph notation required training to be understandable and useful.

4.2 Funding agency case work

The organisation, Dreyers, is a fund that distributes grants for the furthering of architects and lawyers in danish society. They distribute grants for travel, education and projects to architects and lawyers. (Dreyersfond.dk, 2017) We received a DCR graph of Dreyers application handling process. This process is centred on the reception of an application for a grant which is then processed by a caseworker, lawyers, board members and an accountant. The use of DCR graphs as a tool for representing their process was created by Exformatics who also supplies their Electronic Case Management (ECM) system.

To present the GDPR formalisation for the case worker, we merged (by hand) the GDPR fragments with the business process of Dreyers fund. We then used the simulation feature of the DCR tool to present to the case worker how the business processes at Dreyer was influenced by the GDPR. During the simulation, the case worker discovered the possible new activities she needed to handle during her daily work, such as the withdrawal of consent. An example swimlane from the simulation is shown in Figure 4.2.

5 Conclusions and Future Work

The case study revealed both possible advantages and challenges using the DCR Graph notation and the DCRGraphs.net tool for digitalising the GDPR. On the positive side, the declarative DCR Graph notation supported seamless merging of the GDPR constraints with the existing business process of the Dreyer foundation. Also, the DCRGraphs.net tool allowed for easy simulation of the resulting DCR constrained business process jointly with the case worker. However, the graphical DCR notation for constraints posed challenges for consultants and case workers. Future work will be to work on a textual presentation of constraints, which would allow a representation of the GDPR constraints that resembles the representation in the regulation, which we believe would make it

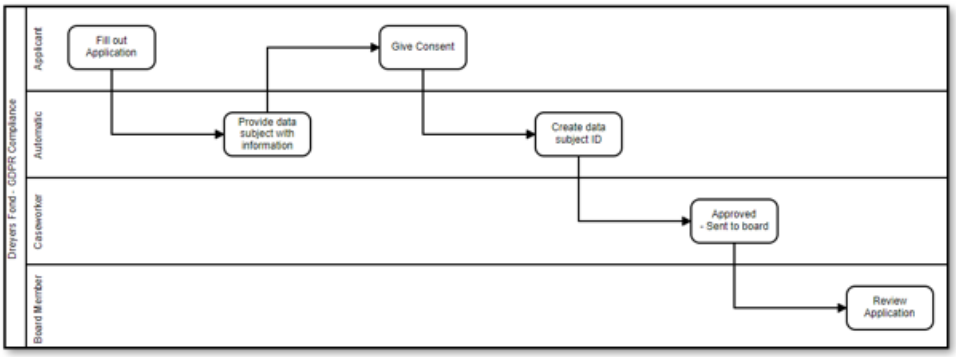

Fig. 4. Example swimlane generated by simulating the Dreyer business process merged with the GDPR formalisation.

more accessible to lawyers and case workers. This will be tested with systematic studies of case workers and lawyers reading and modifying models. We are also working on methods for automating the merging of GDPR constraints and business processes based on data dependency diagrams.

References

1. Søren Debois, Thomas T. Hildebrandt, Tijs Slaats, and Morten Marquard. A case for declarative process modelling: Agile development of a grant application system. In *EDOC Workshops '14*, pages 126–133. IEEE Computer Society, 2014.
2. 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). *Official Journal of the European Union*, L119:1–88, April 2016.
3. Thomas Hildebrandt and Raghava Rao Mukkamala. Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs. In *Post-proceedings of PLACES 2010*, volume 69 of *EPTCS*, pages 59–73, 2010.
4. Raghava Rao Mukkamala. *A Formal Model For Declarative Workflows: Dynamic Condition Response Graphs*. PhD thesis, IT University of Copenhagen, 2012.