Contents

[1. Introduction](#_gjdgxs)

[2. Details on GDPR & DCR](#_30j0zll)

[3. Description of the case process](#_17dp8vu)

[4. Reflection](#_vx1227)

[5. Conclusion](#_3l18frh)

[Table 1 Graphical representation of activities](#_tyjcwt)

[Table 2 Graphical representation of relations](#_2s8eyo1)

[Figure 1 DCR of the process](#_26in1rg)

[Figure 2 DCR model of giving the consent for main purposes](#_35nkun2)

[Figure 3 DCR model of getting assistance from the controller](#_3j2qqm3)

[Figure 4 DCR model of termination of relationship](#_1ci93xb)

[Figure 5 DCR model of blocking request](#_49x2ik5)

[Figure 6 DCR model of data portability, information modification and the right to be forgotten](#_3o7alnk)

[Figure 7 DCR model of giving and withdrawing consent for opinion-research institutes](#_ihv636)

[Figure 8 DCR model of data breach; no subprocess spawned](#_1hmsyys)

[Figure 9 DCR model of data breach; One sub-process is spawned](#_2grqrue)

[Figure 10 DCR model of giving consent for main purposes. The activities in group Mandatory are available](#_1v1yuxt)

[Figure 11 DCR model of giving consent for main purposes. The activities in group Mandatory are blocked](#_3tbugp1)

[Figure 12 DCR model of Data breach. Two sub-process are spawned](#_46r0co2)

[Figure 13 DCR model of the entity Data breach. Two sub-processes are spawned with StartNotification added in the figure](#_111kx3o)

# Introduction

In the past years, more and more people have been using the internet to accomplish their daily activities, which ranges from playing online video games to paying taxes and shopping, but they also use it for some activities that were done on their own computers and are now done on far located servers (storage of data in the cloud and editing documents on Google docs are good examples of that), these new ways of computing raise many questions about how our data is processed and stored. More than 250 Million people now use the internet on a daily basis in Europe, it is thus increasingly important to protect these users and their data from misuse by the companies who they have given it to which could use it for purposes other than what the user consented to or by criminal organizations who could sell user’s data or try to blackmail them in case it would contain sensitive information.

When looking at the recent history, we can see that many data breaches happened in the last years, from the Sony security breach in April 2011 which compromised the accounts of 77 million users to the Yahoo! breach which happened in late 2014 but was only revealed to the public late September 2016. The compromised information included names, email addresses, dates of birth and telephone numbers of over 500 million people.

These problems related to their data worries many EU citizens. When asked 71% of Europeans said that they feel that there is no alternative other than to disclose personal information if they want to obtain products or services and only 15% feel they have complete control over the information they provide online; one in three people (31%) think they have no control over it at all. [reference]

That is why the European Commission has proposed as early as 2012 the General Data Protection Regulation (GDPR), which was adopted on the 27th of April 2016.

The GDPR has set as goal to give people confidence in the online services they are using by having more transparency about how and why their data is handled. Some of the main issues addressed in the new regulation are the need for the individual’s clear consent to the processing of the personal data, the company must ensure that they give data subjects clear and transparent notice of the ways in which, and purposes for which, their personal data will be processed, the right to data portability from one service to another, the right to erasure and rectification and many other new rights, all of which will be explained in detail in the latter sections. The GDPR is a modernization and a harmonization of the actual data protection laws. It will take effect on the 28th of May 2018 and will replace the data protection directive (officially Directive 95/46/EC) from 1995.

The new data regime will be applied to all companies offering goods and services to EU residents or monitor their behavior which means it will also be applied to non EU companies. In fact, the new regulation will make it easier for non EU companies to enter the European market by having a harmonization of the regulation throughout the EU, instead of having them to comply with a different set of laws in each country. This is a big change from the last framework, under this regime the important factor is where the company’s activity occurs not its location.

There are strict penalties for companies not complying to the laws, they vary from a simple written warning in case of first and unintentional noncompliance to different fines.

Data controllers have to ensure that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures". Data controllers can be fined to the height of 05% of their worldwide turnover (or 20 Million € whichever is greater).

In contrast if data processors breach their statutory data security obligations, which requires them to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" of their personal data processing, then the most they could be fined is up 02% of their worldwide turnover (or 10 Million € whichever the greater). [11]

Before the new regulation takes effect, each company has to make sure that the way it processes their customer’s data complies with the GDPR. In order to do that, they must first document the different processes and requirements to have an overall view of the system. Then, all data processing activities must be reviewed, and the company has to evaluate whether the EU regulation applies to that activity, this will allow companies to figure out which data processing activities needs to be changed, and furthermore how to implement these changes in order to comply with the regulation. The GDPR applies only to activities which process personal data. Personal data means any information to an identified or identifiable person, who can be identified either by name, social security number, location data or other. The company also has to ensure that they have a lawful basis for each personal data processing activity. A lawful basis could be an explicit consent given by the data subject, a legal obligation to perform such processing, or that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

What we have tried to do in this project is taking a real company as an example to illustrate how the new regulation will affect its activity and the measures it will need to take in order to comply with the GDPR, this example is Rejsekort A/S. We have therefore found how they use their client’s data in a document released by them in 2014[6].

Rejsekort is an electronic ticket system for the public transportation in Denmark, it has recently completely replaced the old klippekort system. The system needs some personal data given by the users in order to function correctly. When a person registers as a new customer, they will have to send their name and optionally a photo to get the Rejsekort. In other situations, the user’s personal data will be processed without him or her explicitly asking to for example when reloading their personal card, their personal data will be sent to our partners in order to carry out the task. The personal data is processed with the consent of the data subject. All the uses of the personal data are documented and presented to the user before registering, and an explicit consent has to be given by him or her in order to process that data.

# Details on GDPR & DCR

* 1. GDPR

One of the main points in the GDPR is that the controllers are required to get consent for the processing of the personal data for each purpose they will process it. The purpose should be explicit and unambiguous. The main idea is to give the data subject clear overview of what kind of data is collected and for what purposes. On the other hand, getting consent for each purpose gives the data subject flexibility not to give the consent for all the different ways the company wants to process his or her data, especially if it would not be an obstacle for the services provided by the controller. An example of this is the opinion research institutes which can get access to personal data for opinion surveys. The consent can also be withdrawn later.

Another focus in the GDPR is that the collected data should be used only for the purposes for which they are collected. The processing of data for other purposes is possible only if they are compatible, which would require further analysis. Using data for any other non-specified and non-compatible purposes would mean violation of the regulation law. [7, page 9, (50)]

With the new regulation the controller is expected to require only a minimum set of personal data that are necessary for achievement of the purpose. Collecting unnecessary ones should be avoided.

Collected data should be stored as long as it has a purpose. If the purposes are achieved and part/all of the collected data is no longer necessary, then they no longer should be kept.

Before processing all the personal information should be accurate and up-to-date. [7]

Here are some concepts included in the GDPR that we have chosen not to cover explicitly in our model.

***Data protection by design and default:*** The protection of personal data has to be as much as possible designed into the system, turned on by default, and not left to the user to activate. It includes many different concepts such as data minimization, data pseudonymization and encryption.

***Data minimization:*** Is a concept stating that the company should not process more information that it actually needs to achieve the purpose for which the data was given by the data subject.

***Data pseudonymization:*** the regulation defines it as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.” it is thus the process of separation of data from direct identifiers, which would be kept separately. It helps reducing the risk for the data subject.

***Data anonymization:*** making the set of data in such way that no individual can be identified by any way, either by encrypting or removing personal identifiers.

***Appoint a DPO:*** appointing a data protection officer is not a legal obligation in every case. Data protection officers must be appointed for public authorities and companies where the main activity involve “regular and systematic monitoring of data subjects on a large scale” or processing of large data sets containing special categories of personal data such as ethnicity, religious or philosophical beliefs, also called sensitive personal data. It is however a good practice to appoint a person who is responsible for assessing the company’s processing of personal data

**The data subject has the right not to be profiled** **:** “1. 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. … Paragraph 1 shall not apply if the decision … is based on the data subject's explicit consent.” [7, Article 22, paragraph 1,2]. As it is stated, the data subject can object to any automatic processing, including profiling, except the case, when the consent is given. Profiling could be used for price discrimination, targeted servicing or credit rating. the GDPR has the same requirements about profiling as Directive 94/46/EC with some minor amendment and the addition that profiling is possible if the consent is given.

* 1. DCR

Here, we will represent and describe in more details DCR graphs that we used to model our process. DCR (Dynamic Condition Response) graph is a declarative, constraint-based business process modeling language. In the declarative languages like DCR all the flows in a process are implicitly defined, based on the constraints between the events. The number of the flows is restricted only by these constraints. [1] [3]

A DCR graph is a directed graph, where the nodes, drawn like boxes, represent the events, or activities, and the arrows represents the relations between the events. The representation of any process using DCR notations is simply called graph. Each DCR graph represents a process, which includes at least one activity.

The activities play a main role in DCR graphs, they represent an action to be done. They are connected by one or more edges, which represent the constraints between them. Each activity allows nesting, explained later in this section. An activity can be in one of three states – executed, pending or included/excluded and it could be only in one state at a time. Details and graphical representation of the activities and their states is given in table 1

There are 4 *relations* between activities defined in the first version of DCR graph – condition, response, inclusion, exclusion [2]. The relation starts from an activity and ends in another activity or in the in the activity itself. Later the graph is extended with the notion of milestone. To explain the meaning of the relations we will use the notation of DCR Workbench for simplicity. We also used the visual tool from DCRgraph.net, the model can be found in the Appendix.

The graphical representation of the relations can be seen in table 1:

* A condition A -[k]->\* B represents the constraint that for event B to happen, A should be executed at least k steps before B [5]. When there is no requirement for numbers of the steps, then this condition can be represented in the following format: A -->\* B. If A is excluded, then A is no longer requirement for B. After re-inclusion of A, the number of the steps will not be reset to k.
* A response A \*-[d]-> B sets an effect that when A happens, B becomes pending and should happen at last d steps after the execution of A [5]. Here *d* imposes fixed deadline, but in its absence the event B is obligated to happen eventually, without any concrete deadline. It the case of the latter the relation could be represented as follow: A \*--> B. The deadline can’t be zero i.e. can’t happen immediately.
* An exclusion A --% B is an effect that when A happens, B is excluded and can’t be executed [5]. When B is excluded, it is no longer condition. If B was a pending obligation before exclusion, it need not happen after exclusion, unless re-included.
* An inclusion A--+ B is an effect that when A happens, B is included. Now B can be executed. If B is condition for another activity, after re-inclusion it becomes valid.
* A milestone A --<> B is a constraint that for event B to happen A should be not pending or excluded [5]. So If A is included, but not pending, B can also happen.

There is one more relation called “s*pawn*”, but unlike the other five relations it specifies creation of sub-process than setting a constraint. The spawn relation is only possible between an activity and a sub-process, but not between two activities or to the same activity.

Graphs allow assigning a *role* to the events, so that the actors, responsible for execution of an event, can be noted.

*Nesting/Grouping* of the activities is added in one of the later extensions. The nesting represents grouping a set of related events, such that the relation from an event to the nesting node is valid to all grouped events.

The notion of *spawned sub-processes* is one of the other extensions to the DCR graph. A DCR graph represents a business process, but each process can include sub-processes. Every sub-process can be either:

- single-instance subprocess, meaning a process embedded in the main process, or

- multi-instance subprocess, that can be spawned to run independently of the main process [4].

The graphical representation of the activities in the two tools - the visual tool and DCR workbench - and more details are available in Table 1 below.

*Table 1 Graphical representation of activities*

|  |  |  |  |
| --- | --- | --- | --- |
| DCR workbench | DCR.net visual tool | DCR workbench, code | Description |
| Activity; included | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_itu.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity.PNG | “Activity” | Activity can be executed only if it is included and the constraints like condition and milestone are fulfilled. When added the activity is included by default. In the visual tool, this state can set by check “included”. |
| Activity; excluded | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_excl_itu.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_excluded.PNG | % “Activity” | After exclusion, an activity will be again available to be executed, when it is included. Exclusion of an activity affects the relation going out from that activity. If the activity is a condition for another, after exclusion it is no longer valid. The same is valid for milestone. |
| Activity; Pending | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_pending_itu.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_pend.png | !”Activity” | An activity will occur in pending state after another activity has executed and there is response relation between them. The pending activity is expected at some point to be executed, but the execution is no longer required if it is excluded in meanwhile. |
| Activity; executed | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_executed_itu.png | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_executed.png | :”Activity” | An activity could be executed several times except it has an exclusion relation to itself. It this case it will be excluded after the first execution. |
| Nesting/Grouping | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Group_itu.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Nesting.PNG | Group “Group name” {  “Activity”} | Grouping in DCR Benchmark has the functionality of Nesting in the visual tool. A relation from the group / nesting is equal to putting relation to and from each of the compounding activities of the group. |

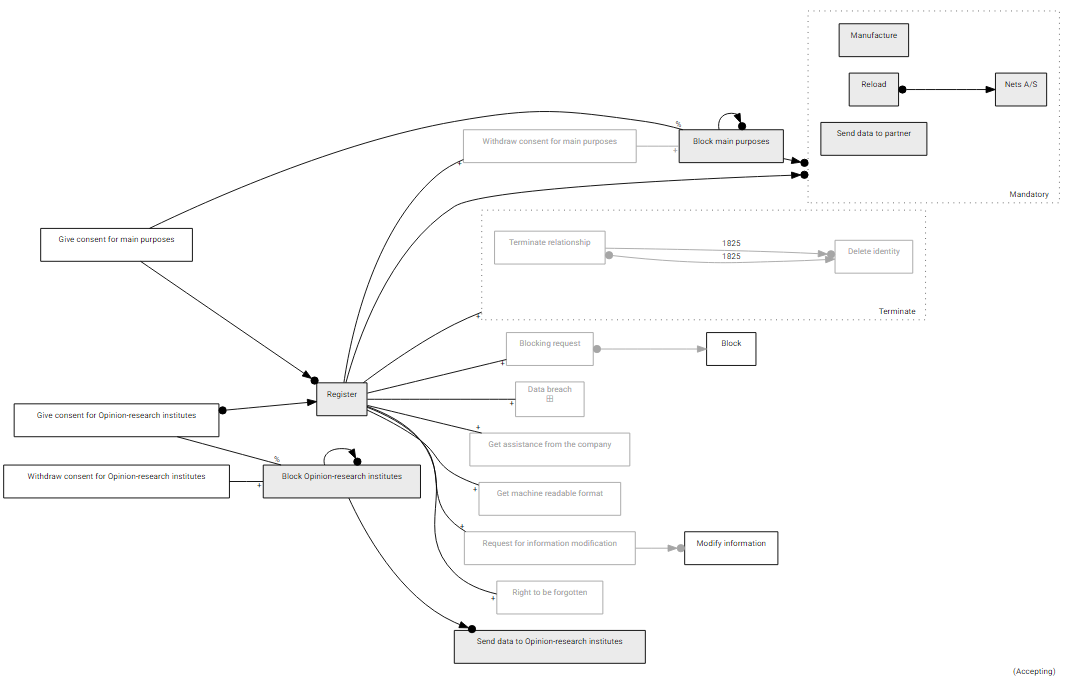
In Table 2 is shown the graphical representation of the relations between the activities and sub-processes.

*Table 2 Graphical representation of relations*

|  |  |  |  |
| --- | --- | --- | --- |
| Relation; Condition | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Condition.PNG |  | -->\*  -[k]->\* | “A condition between two activities ensures that the second activity cannot be executed unless the first is excluded or has been executed at least once.” Timed version is also included. |
| Relation; Response | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Response.PNG |  | \*-->  \*-[k]-> | “A response, or goal, ensures that once the first activity has been executed the other activity becomes a goal, that must eventually be executed or excluded”. Timed version is also included. |
| Relation; Include | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Includes.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Include_itu.PNG | -->+ | “The include relation includes other activities upon execution” |
| Relation; Exclude | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Exclude.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Exclude_itu.PNG | -->% | “The exclude relation excludes other activities upon execution” |
| Relation; Milestone | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Milestone.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Milestone_itu.PNG | --<> | “The milestone relations block the second activity if the first is currently a goal (response) and included.” |
| Relation; Spawn | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Spawn.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Spawn_itu.PNG | “Activity” {  } | “The spawn relation spawns a new sub-process” [4] |
|  |  |  |  |

# Description of the case process

In this section, we will model how GDPR requirements are expected to be applied in our case “Modeling the GDPR requirements for data protection within Rejsekort A/S”, Figure 1.



*Figure 1 DCR of the process*

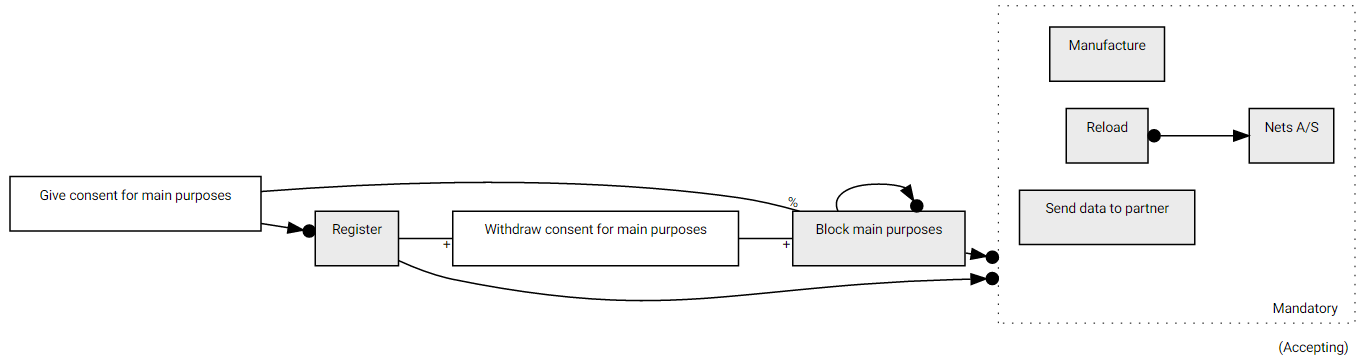
The GDPR keeps using the same definitions for “controller” and “processor” with almost no changes. According to GDPR, "Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.” [7]. And "Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.” [7]

In our case the controller is Rejsekort A/S but is also the processor. A careful look in the documentation [6] shows that there are other companies included in the data processing. One of them is Nets A/S, in which system the customer payments are executed.

The GDPR requires the controller to have lawful basis to process personal data. One of the lawful basis is the consent given by data subject. The consent should cover all the purposes of the processing. This requires Rejsekort A/S to specify and document the purposes of the processing of its customers’ personal data as well. As the GPRD underlines, the personal data should be collected for explicit purposes and the consent should be explicit [7], it must require the consent for the services provided by Rejsekort A/S to be distinguished from the consent for marketing purposes. In the section 2 of [6] it is declared that opinion research institutes can have access to the following information about the customer: “name, address and e-mail address”. The given personal information is sufficient to identify natural persons and since the processing of the data for opinion research institutes is separate from the processing to provide the main services, we decide to split the consent in two different consents: consent for main purposes and consent for opinion research institutes.

Consent for main purposes – going through [6] we considered to put the following purposes in one group, called by us “main purposes” – manufacture the card, reload operations of the balance, send data to partner/affiliated companies. They form the core of the services, provided by Rejsekort A/S, and are closely related to each other.

Each customer using the Rejsekort system should get a traveling card. To produce a card, the manufacturer gets the name and possibly the photo of the customer, depending on the type of the card [6]. On the other hand, the customer needs to reload his or her balance, using the reload automats on the train stations or the company’s website. All payment operations are carried out by Nets A/S which receives the data from Rejsekort A/S to finish the payment operation. In [6] is stated that “Employees in Rejsekort A/S and the affiliated transport companies, whose job it is to serve you as a customer and process your personal data, have access to the collected personal data.” From this statement it is clear that not only the employees of Rejsekort need access to personal data, but the affiliated companies could also get the personal data. We decide to put all the above activities in a group, called main purposes. Any other purposes, which are part of the core functionality of the Rejsekort A/S system, could be specified and added to this group. The DCR model of giving consent for main purposes is shown in Figure 1.



*Figure 2 DCR model of giving the consent for main purposes*

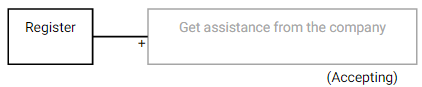
In Figure 2 the following activities are illustrated – “Give consent for main purposes”, “Block main purposes”, “Register” and the group item “Mandatory”. The activity “Give consent for main purposes” models giving a consent for the main purposes by the data subject, which is a requirement before to start processing. “Register” represents the act of getting registered in the system. Here the customer fills in his/her personal data in the Rejsekort A/S system, after which Rejsekort, as a controller, can begin processing the given personal data. “Block main purposes” and “Withdraw consent for main purposes” are related to withdrawing a consent that will be discussed later in this section.

“Mandatory” encapsulates the main purposes mentioned above. The “Mandatory” group includes the activities “Manufacture", “Send data to the partner” and “Reload” with response relation to “Nets A/S”. The activity “Manufacture” describes the production of the traveling card. “Reload” represents loading the traveling card with desired amount. Since all the payments in Rejsekort A/S is proceed through the Nets A/S system, the event “Nets A/S” represents the usage of that system. “Send data to the partner” depicts sending the data to the affiliated companies.

In the beginning neither “Register”, nor the activities in “Mandatory” can be executed, because they are blocked - “Register” is a condition for “Mandatory”, and “Give consent for main purposes” is a condition for “Register”. The graph in the figure above is in that initial state. The execution of “Give consent for main purposes” excludes “Block main purposes”, because of the exclusion relation between them, and so “Block main purposes” is no longer a condition for “Mandatory”. There lefts the condition “Register”, where the customer fills in his personal data. After the execution of “Register”, the activities in “Mandatory” are allowed to be executed. The initial state of the graph above complies with the expectation that a customer should give his or her consent before to be able to “Register”.

GDPR, like the previous directive, guarantees the right of the data subjects to withdraw their consents [7]. The withdrawing of a consent make it is impossible for the controller to use the personal data later for the purposes for which they were collected. To illustrate this, we will use the same model in Figure 1. As mentioned above, the two activities “Withdraw consent for main purposes” and “Block main purposes” are part of the withdrawing of the consent. The activity “Withdraw consent for main purposes” illustrates withdrawing the consent given to process the personal data. “Block main purposes” doesn’t depict some activity of the data subject or the controller and acts like a switch. The “Register” activity has *include* relation with “Withdraw consent for main purposes”. The latter has the same relation with “Block main purposes”. “Block main purposes” excludes itself when the consent is given, and gets included (becomes again a condition for “Main purposes”) after withdrawing the consent. The initial state of “Withdraw consent for main purposes” is excluded – it cannot be executed before giving the consent. When “Withdraw consent for main purposes” is executed, it re-includes the event “Block main purposes”. Since the latter is a condition for “Mandatory” group, after the its re-inclusion, “Block main purposes” again becomes a condition for “Mandatory” group and the group gets blocked.

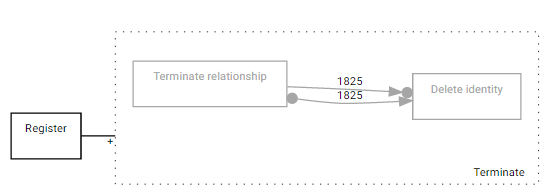
Another area related to the rights of the data subjects extended in the GDPR is the right of the data subject to get support from the controller to exercises his/her rights. The Directive 95/46/EC doesn’t obligate the controllers to give effect to the rights of the data subjects. With the new change, the recommendations of the Directive to help the data subject becomes an obligation that the controller should comply with. This is reflected in our model and can be seen in Figure 2. The controller should take into account all the new rights given to the data subject and implement appropriate measures to reflect their expectations. This could include training of the employees to respond as fast as possible to data subjects’ requests. [8]



*Figure 3 DCR model of getting assistance from the controller*

The Figure 3 includes two events – “Register”, which is explained before, and “Get assistance from the company”, which depicts the right of the customer to get assistance to exercise his/her rights. It is excluded by default and can be included when the customer is registered. After the inclusion “Get assistance from the company” can be executed.

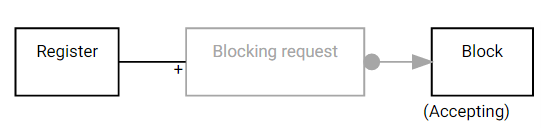
Article 13 of [6] requires the controller to inform how long the personal data will be kept. Rejsekort A/S already complies with this rule and in [6] it discloses that keeps this information for five years after the termination of the customer relationship. This is modeled and illustrated in Figure 3.



*Figure 4 DCR model of termination of relationship*

In Figure 4 there are three activities – “Register”, “Terminate relationship” and “Delete identity”. “Terminate” and “Delete identity” are in a group, called “Terminate”. “Terminate relationship” represents stopping to be a customer of Rejsekort A/S. “Delete identity” describes the erasure of all the collected data. “Terminate” group is by default excluded, because it can’t be executed before “Register”. The activities “Terminate” and “Delete identity” are also excluded. The execution of “Register” re-includes the group “Terminate” that on the other hand leads to re-inclusion of both activities in the group, because a relation with a group is valid for all the activities within the group. The activity “Terminate relationship” has response and condition constraints to “Delete identity”. The execution of “Terminate relationship” will require a pending response within 1825 days. The number 1825 days is equal to five years. Since none of the tools allow specifying time units, here and in the other figures, where the constraints are timed, we will use days. Beside the response, there is also a condition constraint that requires “Delete identity” to be executed at least 1825 days after “Terminate relationship” is triggered. The combination of these two relations has the effect that “Delete identity” should be executed exactly after 1825 days - neither earlier, nor later, as we expect. So as the model above also behaves, the personal data can’t be deleted before 5 years has passed after the termination of the relation.

Here we will show the blocking process, described in [6]. A travel card can be blocked either by its owner, or by the staff of Rejsekort A/S. The owner can block it in case of lost to prevent further misuse with the card. The reasons of blocking the card by the staff is pointed in [6]. One of the reasons could be that the customer has unpaid debts. In this case beside blocking the card, the customer also would be transferred to Customer Register. In both of blockings the card becomes no longer valid and can’t be used. We model both of the cases with one DCR model that is shown in Figure 4.



*Figure 5 DCR model of blocking request*

In Figure 5 there are 3 activities – “Register”, “Blocking request” and “Block”. “Register” is the same activity from the previous graphs. “Blocking request” depicts the request of the owner for blocking, and “Block” - the process of blocking, which could be executed directly by the employees of the controller because of an unpaid debt or as a result of the request of the customer. “Blocking request” is excluded by default and can’t execute before “Register”. There is an *include* relation between “Register” and “Blocking request”, which means that when “Register” is executed “Blocking request” will be re-included and will be available to be triggered. The relation between “Blocking request” and “Block” is of type response. This means that after the execution of “Blocking request”, “Block” becomes a pending response. The deadline is not specified, so it could be triggered at any time. When the card is blocked the user shouldn’t be able to use the system of Rejsekort A/S. This would mean that some of the activities are no longer valid e.g. “Reload” (“Reload” is no longer valid, since the card is blocked). But we decide not to extend the graph with more constraints to keep it simple.

Figure 6 represents 3 different activities that all has a relation with “Register”. ”Get machine readable format” also called data portability. It means the ability of the user to get all his data from the online service he is using in a format that is compatible with other platforms, it requires common technical standards to allow the transfer from one data controller to another. "Controllers must make the data available in a structured, commonly used, machine-readable and interoperable format that allows the individual to transfer the data to another controller." [12]. This makes it easier to the user to have more control over the processed data. The new law could lead to some extra burden in the companies because of the additional expenses to implement a new system, dealing with the requirement. [7, Article 20]

There is also “The right to be forgotten” sometimes called “right to erasure” is the right for the data subject to have his or her data erased and no longer processed under certain circumstances, which include:

- The personal data is no longer necessary to serve the user in relation to the purposes for which the data was collected.

- The data subject withdraws his or hers consent.

- The personal data was unlawfully used.

- The data subject has given his or hers consent as a child, without being fully aware of the consequences.

If a data subject has requested to exercise his or hers right to erasure, and it was evaluated as a legitimate request, the company has to contact all third parties that have gotten the data subjects’ data by the company, and have to delete the data without undue delay

The request could also be rejected if the deletion of the data would diminish the freedom of expression and information of a third party, if the data is processed for public health purposes or the public interest.

And last we have “Request information modification” and “Modify information”. Every user has the right to change the information the company has on him or her, it could be done in order to rectify the information or for any other reason the user sees fit. “Request for information modification” is a condition to “Modify information”, that means that the company will only modify information of its users upon request.



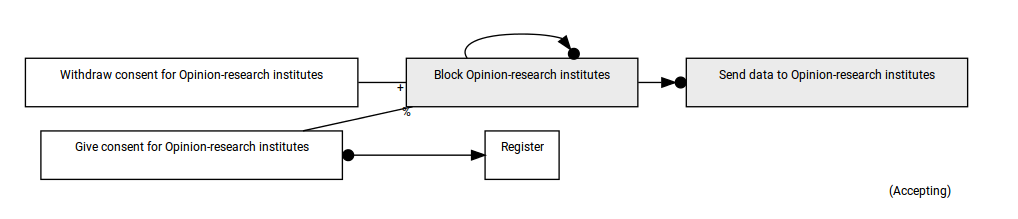
*Figure 6 DCR model of data poratbilty, information modification and the right to be forgotten*

We can see from Figure 6 that “Get machine readable format”,” Request for information modification” and the “Right to be forgotten” are excluded. There is an inclusion relation between the “Register” activity and the mentioned activities, which means that they can be executed only after “Register” has been executed. In this concrete example it means for example that a user cannot exercise his right to be forgotten before he has registered as a client.

In the next figure we have modeled the process of giving and withdrawing the consent for opinion research institutes to process the user's personal data. Rejsekort sends users data to opinion research institutes, the data includes the name, the address and the email. It is done in order to carry out customer satisfaction surveys and improve the user experience. Only users who have agreed to share their data and have given an explicit consent will have their data used. The company will need the explicit consent of the user for each purpose it is going to use the data for. The opinion research institute will delete the received personal data when they have completed their task. This consent is not mandatory in order to use Rejsekort A/S, but if given will help improve the overall service.

The data subject can, if he or she has previously given a consent to the company sending personal data to an opinion research institute, withdraw the consent for that processing without any justification. By withdrawing his or hers consent, the user is ensured that their personal data will not be used in future customer satisfaction surveys.

To model this part of the process, we have used the same “switch” as in Figure 7. In order to execute “Send data to opinion research institutes” the consent has to be given. When the consent is withdrawn it is no longer possible to execute that activity.

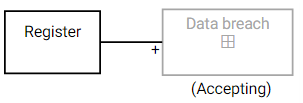


*Figure 7 DCR model of giving and withdrawing consent for opinion-research institues*

We can see from the Figure 7 that we have one activity called “Block opinion-research institutes”, which we have not talked about earlier. This activity is basically a switch.

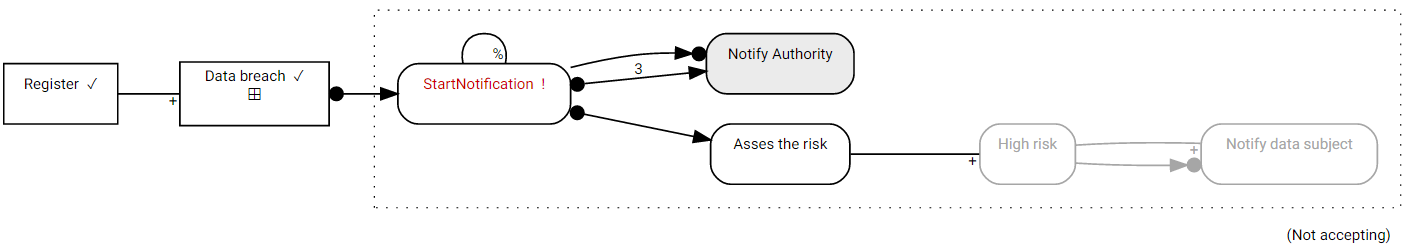
It has itself as condition, which means it cannot be executed. “Send data to opinion research institutes” has “Block opinion research institutes” as condition, and since it cannot be executed the only way to execute the send activity is to exclude the block activity. This can only be done by executing “Give consent”. If the data subject wants to withdraw his consent, it will include “Block opinion research institutes” again, and thus “send data” will not be executable.

Each personal data breach which can lead to material or/and non-material damages to natural persons should be notified to the supervisory authority. When the processor of personal data becomes aware of such a data breach, it is expected to inform the controller immediately. The controller is required to inform the supervisory authority within 72 hours. This notification should include details about the kind of the breach and where it occurred, how many persons are affected, the possible consequences and measures which will be taken to address the security gap. If the data breach poses risks for the rights and freedoms of the natural persons, there appears a necessity for the controller to notify the data subjects as well. In Figure 9 and Figure 9 the DCR model of the data breach in our process is shown.



*Figure 8 DCR model of data breach; no sub-process spawned*

The model in Figure 8 includes the activity “Register” and the sub-process “Data breach” that is initially “closed” – no sub-process is spawned – where “Data breach” represents the data breach of the personal data. The relation between “Register” and “Data breach” is of type *include*. The model after the spawning of the first sub-process can be seen in Figure 9.



*Figure 9 DCR model of data breach; One sub-process is spawned*

The sub-process includes the following activities: “StartNotification”, “Notify authority”, “Assess the risk”, “High risk” and “Notify data subject”. “Notify authority” depicts the act of notifying the supervisory authority, which should be done within 3 days. “Asses the risk” – the process of assessing the risk from the data breach for the rights and freedoms of the data subject. “High risk” – checks if the mentioned risk is high. The activity “Notify data subject” represent notifying the data subject about the likely consequences in the case that the risk is very high. “StartNotification” is a helper event that exclude itself after its execution. It prevents the deadline for notifying the authority to be reset to 3 [days], when another data breach is registered within 3 days. This is explained in more details in section 4. As can be seen in Figure 9 the constraint between “StartNotification” and “Asses the risk” is of type *response.* It is expected the assessment to be done as soon as possible. “Asses the risk” and “High risk” are connected trough *include* relation, this is because by default “High risk” is excluded and it can’t be available for execution before the risk assessment. The activities “High risk” and “Notify data subject” are connected with two relations – *include*, because the “Notify data subject” is by default excluded, and *condition*, because even included “Notify data subject” can’t be executed before “High risk”. For spawning new sub-process as a result of data breaches, the sub-process activity “Data breach” should be executed.

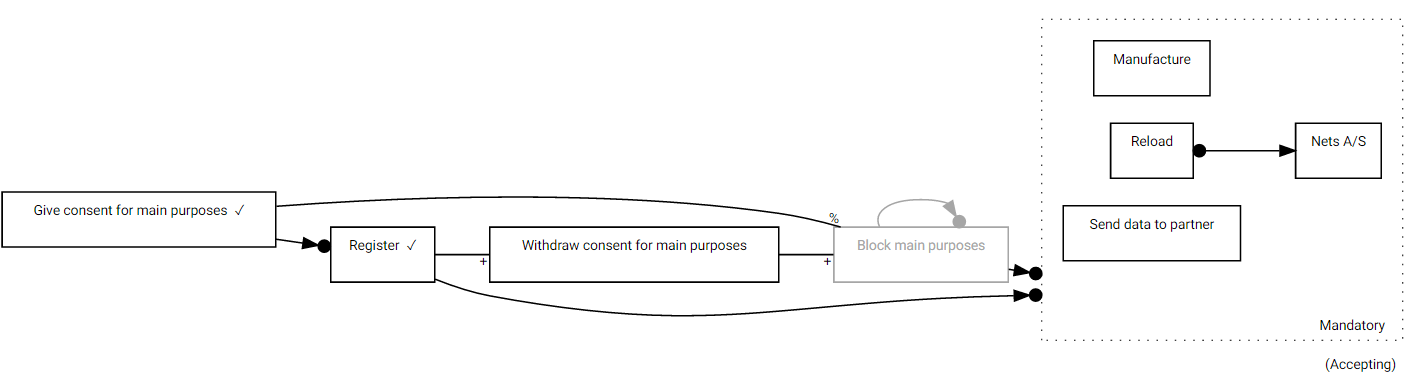
# Reflection

When an imperative approach is used for modeling a business process, we should define all the legal steps to end in another legal step. At each step we specify, which are the next possible ones. A deviation from the predefined path from a step to another step is not allowed. "However, while imperative approaches are a strong concept when it comes to well-defined processes, they lack clarity once an observed behavior allows for flexible execution." [9]

In the declarative approach, on the other hand, each transition from a state to another state is allowed by default, except there is no violation of any of the constraints. Instead of defining the allowed sequences of events, the workflow is described using rules between the events [10]. The flexibility of the declarative way, like DCR, comes from the fact that, when a new constraint between the events arises, it is enough to define it in the graph without explicitly rearranging the flow in the diagram.

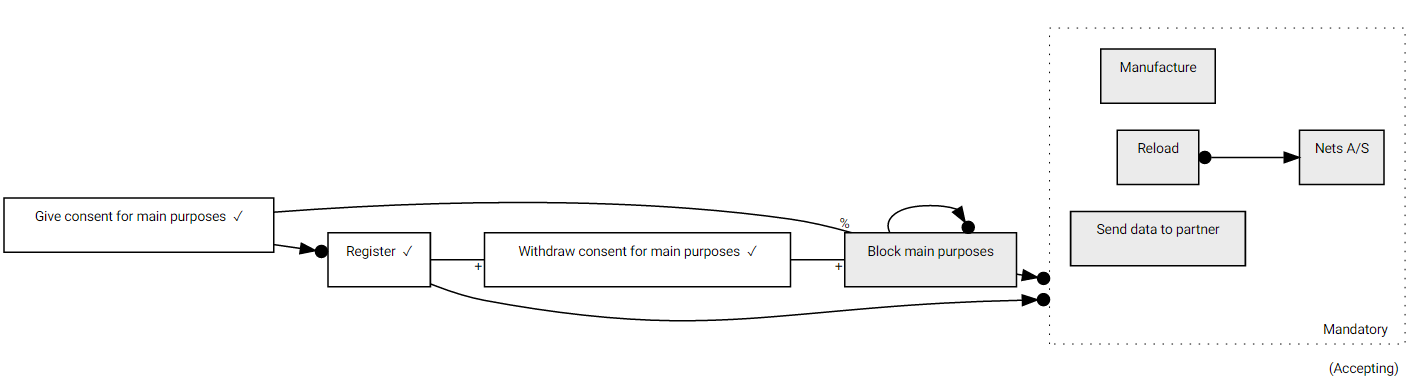
We can see also that using a DCR graph to model our system will be smaller in size comparing if we would use a flowchart. In our example, the user can withdraw the consent for processing his or her data at any time. In order to model that with a flow chart, we have to add an “arrow” from the withdraw activity to all the other activity, which will, if we have enough activities, render the chart unreadable.

In a DCR graph there is no need to put a loop, if some actions would be executed in a cyclic order. The approach here in DCR is to put the appropriate constraints in a way that they allow cyclic execution. The graph in Figure 2 above shows that if the consent for mandatory is not given, the activities in the group “Mandatory” are blocked. This is the initial state of the graph. When the consent is given, the events in the group become allowed - the graph is shown in Figure 10.



*Figure 10 DCR model of giving consent for main purposes. The activities in group Mandatory are available*

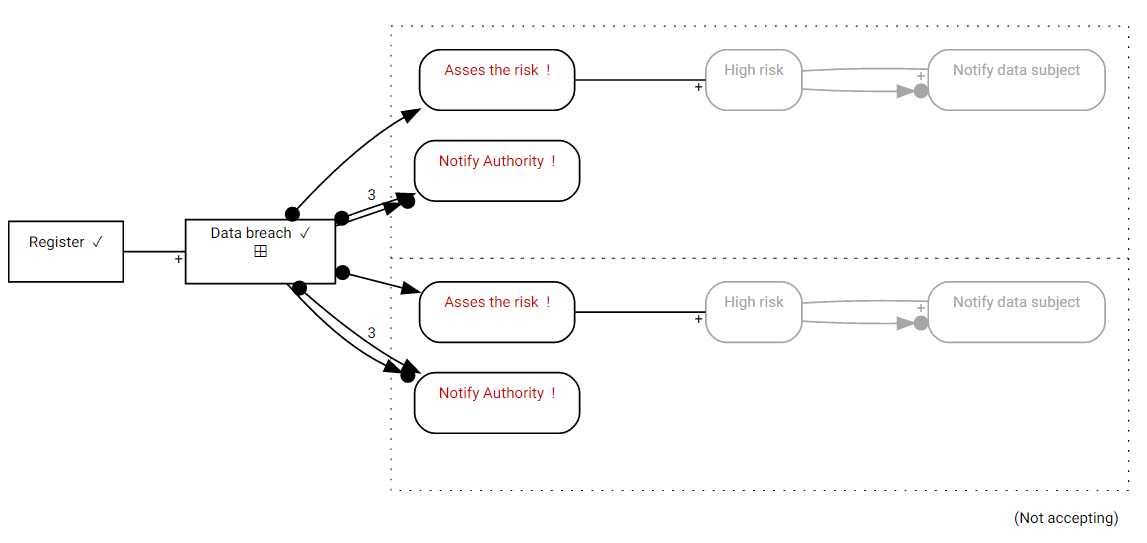
And now if we withdraw our consent, the activities in the group would be blocked and the graph would look like this in Figure 11:



*Figure 11 DCR model of giving consent for main purposes. The activities in group Mandatory are blocked*

In figure Figure 11 we can see that the activities in “Mandatory” are again not allowed because of the existing condition constraint with “Mandatory” group. If we decide to give the consent again, then the only thing to be done is to execute the activity “Give consent for main purposes”. There is no need to define any loops and we don’t change the flow explicitly. The only thing to be done is to add constraints.

We encountered a problem with the sub-process entries in DCR Workbench. When a new sub-process is spawn after an existing one, the deadlines of the pending responses in the existing sub-process are reset to their initial values, which is not correct. We will demonstrate this with an example to the sub-process “Data breach” from our graph. The Figure 12 shows the sub-process item “Data breach” with two spawned sub-processes.

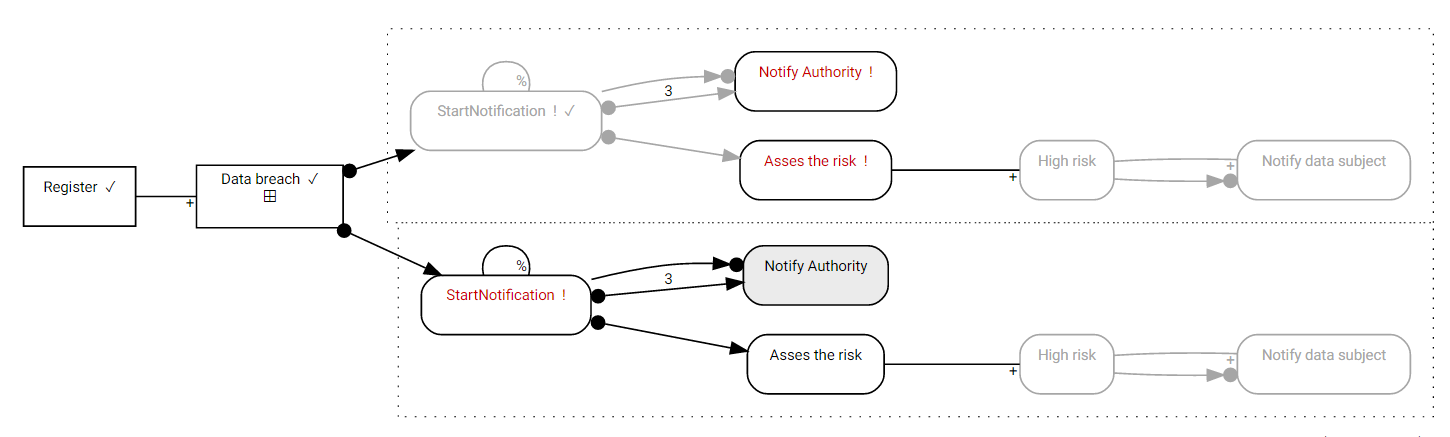


*Figure 12 DCR model of Data breach. Two sub-process are spawned*

During the simulation, the execution of “Asses the risk” for the second sub-process leads to resetting the deadline of “Notify authority” for the first sub-process. For example, if the deadline of the first process is 1, after the execution of the activity “Notify authority” for the second process, both deadlines are set to 3. This is not a correct behavior.

An additional helper event is added to fix this error. The new graph is shown in Figure 13. The event added is “StartNotification” that is put before the activities “Asses the risk” and “Notify Authority”. “StartNotification” has *exclude* relations to itself. After the execution of “StartNotification” it will exclude itself and will be no longer a condition for “Notify authority”, but it will require a pending response with deadline 3 days. When a new data breach will be registered, which means “Data breach” will be executed again, now this will not reset the deadlines of the previous “Notify authority” activities, where “StartNotification” has already executed. “Data breach” will not affect the deadline of “Notify authority”, because “StartNotification” “cuts” the relation between these two events.

To fix this error we recommend not to enforce responses for the sub-processes which are already spawned. If this will be fixed, we will be able to connect directly “Data breach” and “Notify authority” with no need of medium helper event.



*Figure 13 DCR model of the entity Data breach. Two sub-processes are spawned with StartNotification added in the figure*

# Conclusion

The goal of the projects was …

First, we introduced …

Then, we gave details about DCR and GDPR …

After that – went through the new requirements of GDPR and tried to adapt the Rejsekort A/S’s data protection mechanism to the new rules.

We conclude that DCR is appropriate language to model data protection ???requirements …

The goal of the projects was to identify the new rules for data protection in the GDPR and to extend the data protection mechanism of Rejsekort A/S to comply with them whereas modeling of the changes is done with the declarative constraint-based language DCR.

First, we introduced the actuality of the fast ongoing digitalization of the personal data in the last years and the general concerns behind of the wider usage of the data in the business processes. Secondly, we focused on the essential changes in the GDPR that extends the obligations of the controllers and the rights of the data subjects. Third, we explained the main idea behind the DCR graphs, the entries, constructing the graph, and the relations between them, and the graphical representation in the two DCR tools. After that we went through the new requirements of GDPR and tried to adapt the Rejsekort A/S’s data protection mechanism to the new rules. The changes and the extension of the data protection requirements in Rejsekort A/S were modeled and illustrated in figures.

We tried to reflect the extensions that should be made in Rejsekort A/S’s requirements, and doing that we conclude that DCR is appropriate language to model data protection requirements. DCR graph is easy to use and it is also easy to add further constraints to the graph. The latter would be a big advantage in case of extension of the GDPR with new requirements in the future. Thus the graph neither should not be built from scratch, nor any essential big changes should be made in it, but it would be enough to add new constraints for the new requirements.

======

References:

1. T. Hildebrandt, and R. R. Mukkamala. “Distributed Dynamic Condition Response Structures”, IT University of Copenhagen
2. T. Hildebrandt, and R. R. Mukkamala. „Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs”, IT University of Copenhagen
3. G. D. Giacomo, M. Dumas, F. M. Maggi and M. Montali. "Declarative Process Modeling in BPMN", Sapienza Universita di Roma, Italy, University of Tartu, Estonia, Free University of Bozen-Bolzano, Italy
4. http://wiki.dcrgraphs.net/, [Accessed: 11-Dec-2016]
5. In the nick of time … ??
6. Rejsekort A/S, PROTECTION OF PERSONAL DATA – REJSEKORT A/S, Søborg, 2014
7. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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), 2016
8. http://www.whitecase.com/publications/article/chapter-1-introduction-unlocking-eu-general-data-protection-regulation, [Accessed: 12-Dec-2016]
9. J. Prescher, C. D. Ciccio, and J. Mendling, "From Declarative Processes to Imperative Models", Vienna University of Economics and Business, Vienna, Austria, year
10. Pesic, M., Schonenberg, M.H., Sidorova, N., van der Aalst, W.M.P.: Constraint-based workflow models: Change made easy. In: OTM Conferences (1). pp. 77–94 (2007)
11. <http://www.out-law.com/en/articles/2016/may/gdpr-potential-fines-for-data-security-breaches-more-severe-for-data-controllers-than-processors-says-expert/>, [Accessed: 13-Dec-2016]
12. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL>, [Accessed: 13-Dec-2016]

# 6. Appendix

## Dcr.itu.dk + the link

## Report from dcgraphs.net

## ?source documents(?) describing your case process (Rejsekort’s privacy doc)

## Excerpts from the GDPR

// per purpose

“1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’); “[Article 5, page 35]

// the right to be forgotten

“1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or

point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in

Article 8(1).” [Article 17, page 43]

// can get help from the controller

“2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.” [Article 12, page 40]

// data breach

“1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.” [Article 33, page 52]

// machine readable format

“1. 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, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.” [Article 20, page 45]