1. Introduction -  motivate the project
   1. Business process - Business process
      1. The way of sharing of personal data has changed, personal data stored not in remote computers,
      2. Usage of personal data
      3. Access, deal with them
      4. Gaps – should be filled
   2. Background on the GDPR
      1. GDPR, General data protection regulation, is
         1. Data traced back to a person – id, name, IP, DNA
         2. Where is stored, who can access it
         3. Clarify the terms here !!!
         4. 50% - misuse
         5. Almost all – to be informed stolen, lost data
         6. 7/10 – worried that data is used for different purposes
         7. effective control on personal data, right, free and easy access to your personal data
   3. Processes and requirements must be documented - the processing carried out
      1. Which data
      2. Only necessary data
      3. As short as possible
2. Details on GDPR & DCR
   1. GDPR
      1. Companies which want to process personal data should follow principles

One of the main points in GDPR is that the controllers are required to get consent for processing of the personal data per purpose. The purpose should be explicit and unambiguous and the data for which must be collected given purpose should be clearly specified. The aim is to give the data subject clear overview of what kind of data for what purposes is collected. On the other hand, getting consent per purpose gives the data subject flexibility not to give the consent for purposes, for which there is no legal basis and would not be an obstacle for the services provided by the controller. An example for the latter is the opinion research institutes which can get access to personal data for opinion surveys. The consent can also be withdrawn later

The collected data should be used only for the purposes, for which they are collected. 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. (p.9 (50))

With the new regulation the controller is expected to require only a minimum set of personal data, which are necessary for achievement of the purpose and to avoid collecting unnecessary ones.

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.

The right to be erased (“the right to be forgotten”) known from the Data Protection Directive 95/46/EC will be expanded with the new regulation. This law requires deletion of personal data without undue delay. This new law covers besides the cases when the data was processed unlawfully, also the situations where the controller has no longer need of the personal data for the original purposes and no legitimate reason the process them.

(known) Before processing all the personal information should be accurate and up-to-date. (p.5)

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 controller to notify the data subjects as well.

1. Duties of the company – another level
   1. ‘Data protection by design’ and ‘Data protection by default’
2. Rights of the data subjects

GPDR introduces a new right concerning data portability. This is that each person should be able to get structured, machine-readable copy of the data for the purposes pointed by controller, so that the data subject can take and transfer the collected personal data to other service providers. This also makes it easier he or she to have more control over the processed data. (? task carried out in the public interest or in the  
exercise of official authority vested in the controller) (Article 20)

Get assistance from the company to exercises her or his rights

To rectify

Right not to be profiled - “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.” (Article 22, 1.). ??? b) Profiling could be possible if the data subject gives a consent for this purpose.

1. Key changes:
   * + 1. //Consent per purpose
       2. //‘right to be forgotten’
       3. Easier access to your own personal data.
       4. //A right to transfer personal data
       5. easy-to-understand, unambiguous, handle information
       6. //inform you about data breaches
       7. data protection risk assessments,
       8. data protection officers
       9. Data Protection by Design og Default
   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. (3)

A DCR graph is a directed graph, where the nodes, drawn like boxes, represent the events, or activities, and the arrows - 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 main role in DCR graphs that 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 X.

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 same one. Later the graph is extended with notion of milestone. To explain the meaning of the relations we will use the notion of DCR Workbench for simplicity. The graphical representation of the relations can be seen in table X:

* 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, neither the requirement for the steps is valid. After re-inclusion of A, the number of the steps will be reset to k, no matter of the value of k before the exclusion.
* A response A \*-[d]-> B sets an effect that when A happens, B becomes obligated(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 happened eventually, without any concrete deadline. It the case of the latter the relation could 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 not re-included.
* An inclusion A--+ B is an effect that when A happens, B is re-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. [16]

*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 the higher event to 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 sub process, meaning a process embedded in the main process, or

- multi-instance sub process, that can be spawned to run independently of the main process (4).

The graphical representation of the two tools, the visual tool and DCR workbench, and more details are available in table below.

Switch the columns

//Activity – included, excluded, pending, executed

|  |  |  |  |
| --- | --- | --- | --- |
| DCR.net visual tool | DCR workbench | DCR workbench, code | Description |
| Activity; included | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_itu.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_excluded.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_excl_itu.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_pend.png | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_pending_itu.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.png | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Activity_executed_itu.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\Nesting.PNG | D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Group_itu.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. |

Table shows their graphical representation in the tools with description.

Relation – condition, response, include, exclude, milestone, spawn

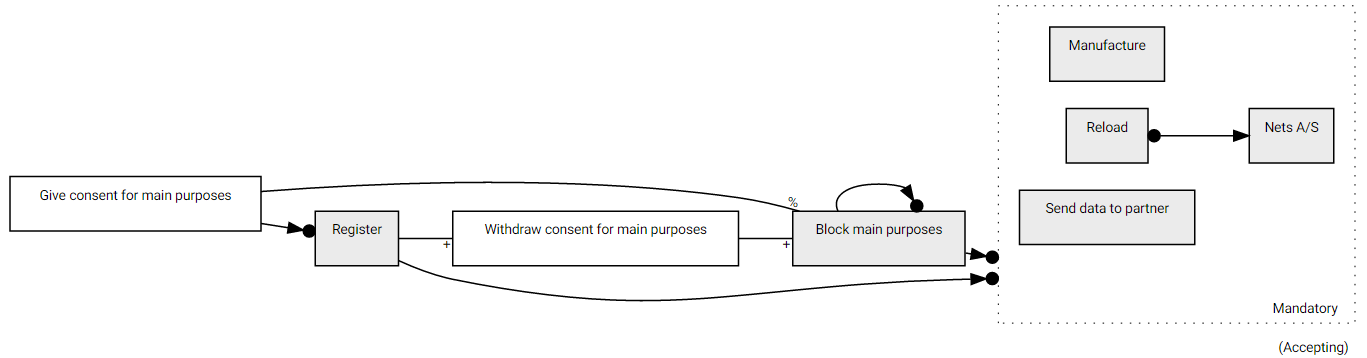
|  |  |  |  |
| --- | --- | --- | --- |
| Relation; Condition | | | |
| D:\ITU_edu\2sem\Critical Systems Project\DCR\pictures\Condition.PNG |  | -->\*  -[k]->\* | “A condition between two activities ensures that the second activity cannot be executed unless the first is excluded or has been executed 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) |
|  |  |  |  |

1. Our process – DCR model, DCR requirements - Modeling the requirements for data protection within the Rejsekort A/S according to GDPR

GDPR requires the controller to have lawful basis to process personal data. One of the lawful basis is the consent given by data subject, that 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 GPRD underlines that personal data should be collected for explicit purposes and the consent should be explicit (7), it must require the consent for providing services 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”. Since the given personal information is sufficient to identify natural persons and the processing of this data are separate from the processing to provide 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 by agreement, send data to partner/affiliated companies, service???. They form the base of the services, provided by Rejsekort A/S, and are closely related to each other. Each customer using the Rejsekort system should have a card. The manufacturer of the card gets the name and possibly the photo of the customer, depending on the type of the card, to produce the card (6). Also the customer needs to reload his or her balance using the reload automats on the stations or the website of the company. All payment operations are carried out in the system of Nets A/S which gets the data from Rejsekort A/S. 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 have access to personal data, but the affiliated companies as well. Although it is not clear from (6) what the concrete purposes of the employees of the partner companies are we decide to put them in the group of main purposes, because they “serve and administer you as a customer”. Rejsekort A/S would be required to specify these purposes later. Any other purpose which is part of the base functionality of the Rejsekort system could be specified and added to this group. The DCR model of giving consent for main purposes is shown in figure X

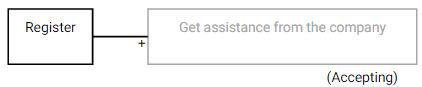


In the figure the following activities are illustrated– “Give consent from main purposes”, “Block main purposes”, “Register” and group item “Mandatory”. The other two activities “Withdraw consent for main purposes” and “Block main purposes” are related to withdrawing a consent that will be explained later in this section. The group entry “Mandatory” encapsulates the main purposes mentioned above. “Mandatory” group includes the activities “Manufacture", “Reload” with response relation to “Nets A/S” and “Send data to the partner”. In the beginning neither “Register”, nor activities in “Mandatory” can be executed, because “Register” is a condition for “Mandatory”, and “Give consent for main purposes” is a condition for “Register”. The graph in the figure is in that state. Execution of “Give consent for main purposes” excludes “Block main purposes”, because of exclusion relation between them, and “Block main purposes” is no longer a condition for “Mandatory”. There lefts the condition “Register”, where the customer fills his personal data in. After execution of “Register”, the activities in “Mandatory” are read for execution. 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”.

Register – give your personal data.

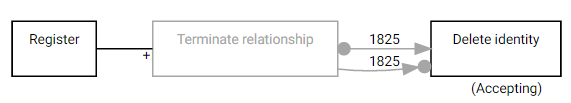
(Rejsekort complies with this) GDPR, like the previous Directive it, guarantees the right of the data subjects to withdraw their consents (7). The withdrawing of a consent make it is impossible for the controller to use the personal data for the purposes for which they are collected. To illustrate this, we will use the same model in figure X. As mentioned above, the other two activities “Withdraw consent for main purposes” and “Block main purposes” are part of the windrowing of the consent. The “Register” activity has include relation with “Withdraw consent for main purposes” and the latter has the same relation with “Block main purposes”. 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 includes the event “Block main purposes”. Since the latter is a condition for “Mandatory”, after the inclusion, it is again a condition for “Mandatory” and that’s why it is blocked. “Block main purposes” is syntactic sugar that excludes itself when the contest is given, and is being included (becomes again a condition) after withdrawing of the consent.

The general data protection regulation expands the right of the data subjects to get help from the controller for exercising their rights. The Directive 95/46/EC doesn’t obligate the controllers to give effect to the rights of the data subjects, but in GDPR it becomes mandatory (7). This is reflected in our model and can be seen in figure X.



The figure X 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 already be executed.

Article 13 of (7) requires the controller inform how long the personal data will be kept. Rejsekort A/S already complies with this rule and in (6) it discloses that it keeps this information for five years after the termination of the customer relationship. This is modeled and illustrated in figure X



? Malik (exclude Terminate rel.) In the figure X there are three activities – “Register”, “Terminate relationship” and “Delete identity”. “Terminate relationship” is by default excluded, because it can’t be executed before “Delete identity”. “Terminate relationship” has response and condition constraints to “Delete identity”. The execution of “Terminate relationship” will require a pending response within 1825 steps. But there is also condition that requires “Delete identity” to be executed at least 1825 steps after “Terminate relationship” is triggered. The combination of these two relations has effect that “Delete identity” should be executed exactly after 1825 steps - neither earlier, not later, which notes the five years’ storage time of the personal data in Rejsekort A/S system after stopping the customer relationship. Here and in the other figures where the constrains are timed, they should be understood as days. This is the reason 5 years to be represented in days.

1. Reflection – the plusses of DCR, the lacks
2. Conclusion

======

References:

1. Distributed Dynamic Condition Response Structures
2. Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs
3. <http://www.diag.uniroma1.it/~degiacom/papers/2015/CAISE15.pdf>
4. <http://wiki.dcrgraphs.net/>
5. In the nick of time …
6. PROTECTION OF PERSONAL DATA – REJSEKORT A/S
7. GDPR