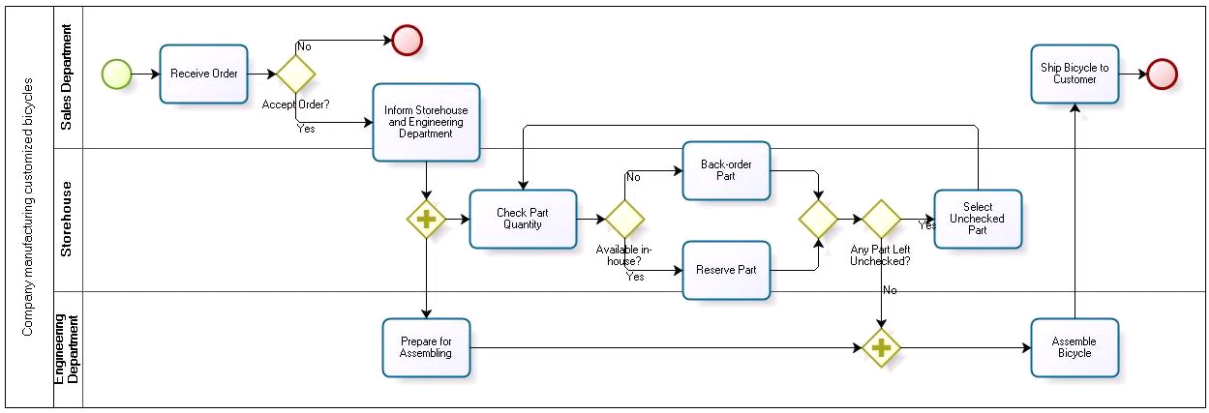
Golden Standard for Bachelor Thesis

1. PET Data

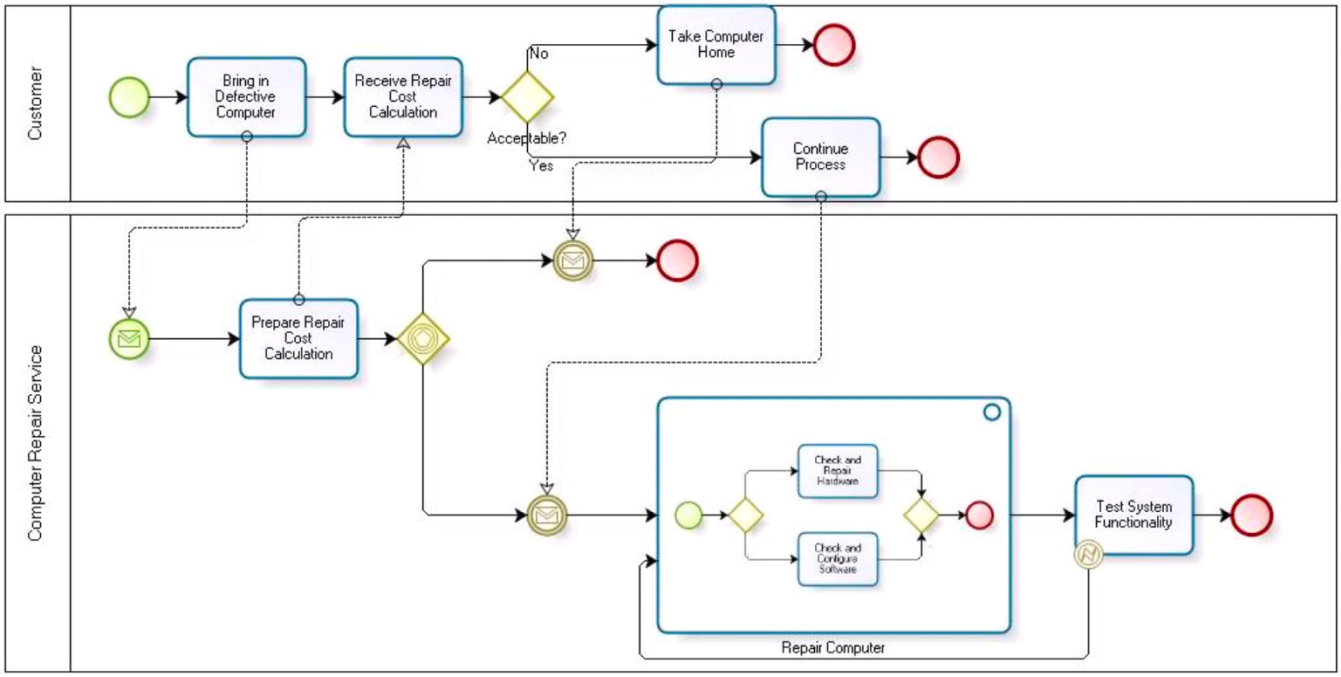
Text 1: Bicycle manufacturing

A small company manufactures customized bicycles. Whenever the sales department receives an order, a new process instance is created. A member of the sales department can then reject or accept the order for a customized bike. In the former case, the process instance is finished. In the latter case, the storehouse and the engineering department are informed. The storehouse immediately processes the part list of the order and checks the required quantity of each part.
If the part is available in-house, it is reserved. If it is not available, it is back-ordered.
This procedure is repeated for each item on the part list. In the meantime, the engineering department prepares everything for the assembling of the ordered bicycle. If the storehouse has successfully reserved **or** back-ordered every item of the part list and the preparation activity has finished, the engineering department assembles the bicycle. Afterwards, the sales department ships the bicycle to the customer and finishes the process instance.



Text 2: The workflow of a computer repair service (CRS)

A customer brings in a defective computer and the CRS checks the defect and hands out a repair cost calculation back. If the customer decides that the costs are acceptable, the process continues, otherwise she takes her computer home unrepaired. The ongoing repair consists of two activities, which are executed, in an arbitrary order. The first activity is to check and repair the hardware, whereas the second activity checks and configures the software. After each of these activities, the proper system functionality is tested. If an error is detected another arbitrary repair activity is executed, otherwise the repair is finished.



Text 3: Hotel Service

The Evanstonian is an upscale independent hotel.

When a guest calls room service at the Evanstonian, the room-service manager takes down the order.

She then submits an order ticket to the kitchen to begin preparing the food.
She also gives an order to the sommelier (i.e., the wine waiter) to **fetch wine** from the cellar and to prepare any other alcoholic beverages.

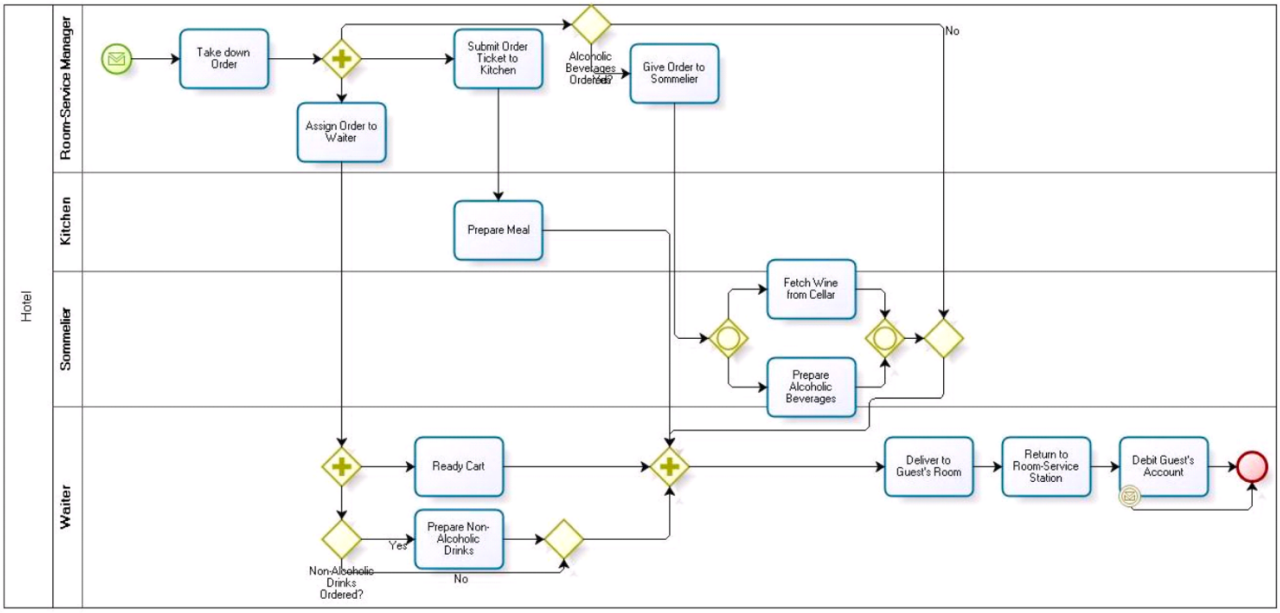
Eighty percent of room-service orders include wine or some other alcoholic beverage.

Finally, she assigns the order to the waiter.

While the kitchen and the sommelier are doing their tasks, the waiter readies a cart (i.e., puts a tablecloth on the cart and gathers silverware).

The waiter is also responsible for nonalcoholic drinks.

Once the food, wine, and cart are ready, the waiter delivers it to the guest's room. After returning to the room-service station, the waiter debits the guest's account. The waiter may wait to do the billing if he has another order to prepare or deliver.



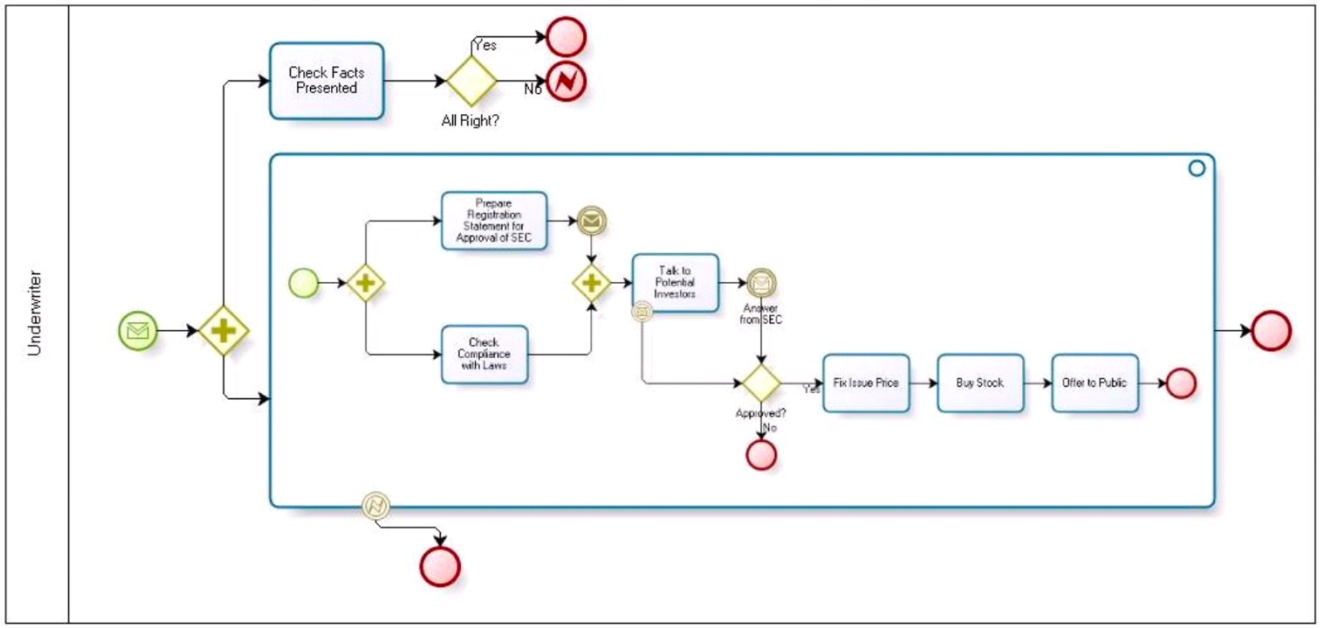
Text 4: Underwriters

Whenever a company makes the decision to go public, its first task is to select the underwriters.

Underwriters act as financial midwives to a new issue. Usually they play a triple role: First they provide the company with procedural and financial advice, then they buy the issue, and finally they resell it to the public.

Established underwriters are careful of their reputation and will not handle a new issue unless they believe the facts have been presented fairly. Thus, in addition to handling the sale of a company's issue, the underwriters in effect give their seal of approval to it.

They prepare a registration statement for the approval of the Securities and Exchange Commission (SEC). In addition to registering the issue with the SEC, they need to check that the issue complies with the so-called blue-sky laws of each state that regulate sales of securities within the state. While the registration statement is awaiting approval, underwriters begin to firm up the issue price. They arrange a road show to talk to potential investors. Immediately after they receive clearance from the SEC, underwriters fix the issue price. After that they enter into a firm commitment to buy the stock and then offer it to the public, when they haven't still found any reason not to do it.



2. Regulatory documents: ISO/IEC 27001:2022

Text 5: 2.1 Monitoring, measurement, analyses and evaluation

The organization shall determine:

a) **what** needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to **ensure valid results**. The methods selected should produce comparable and reproducible results to be considered valid;

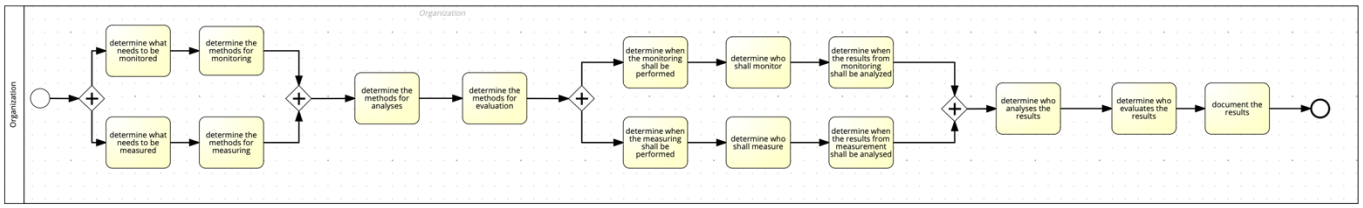
c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analyzed and evaluated; and

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results. The organization shall evaluate the information security performance and the effectiveness of the information security management system.



Text 6: 2.2 Internal Audit

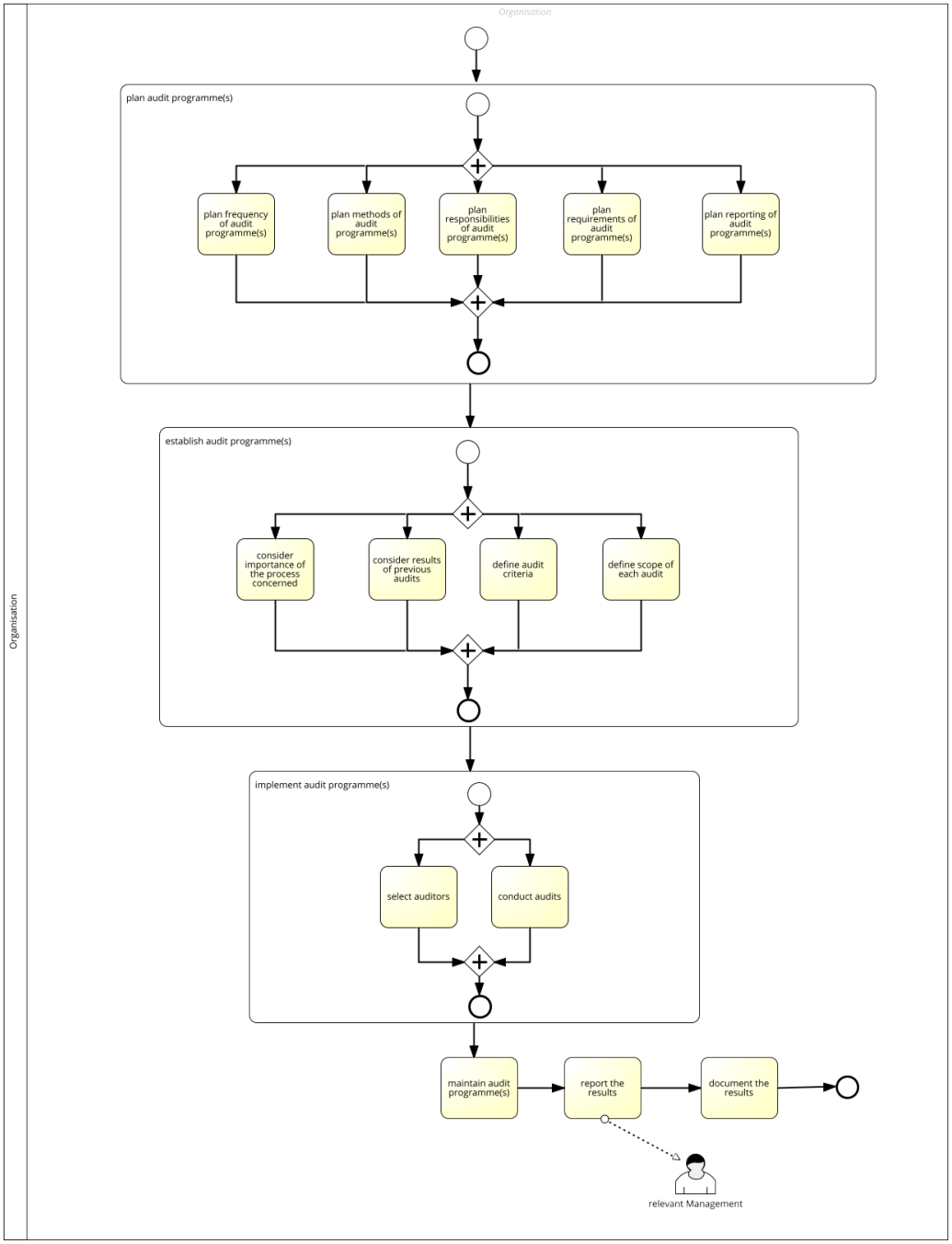
The organization shall **plan, establish**, **implement** and **maintain** an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall **consider the importance of the processes concerned and the results of previous audits.**

The organization shall:

a) define the audit criteria and scope for each audit;
b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.



Text 7: 2.3 Management review

"Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

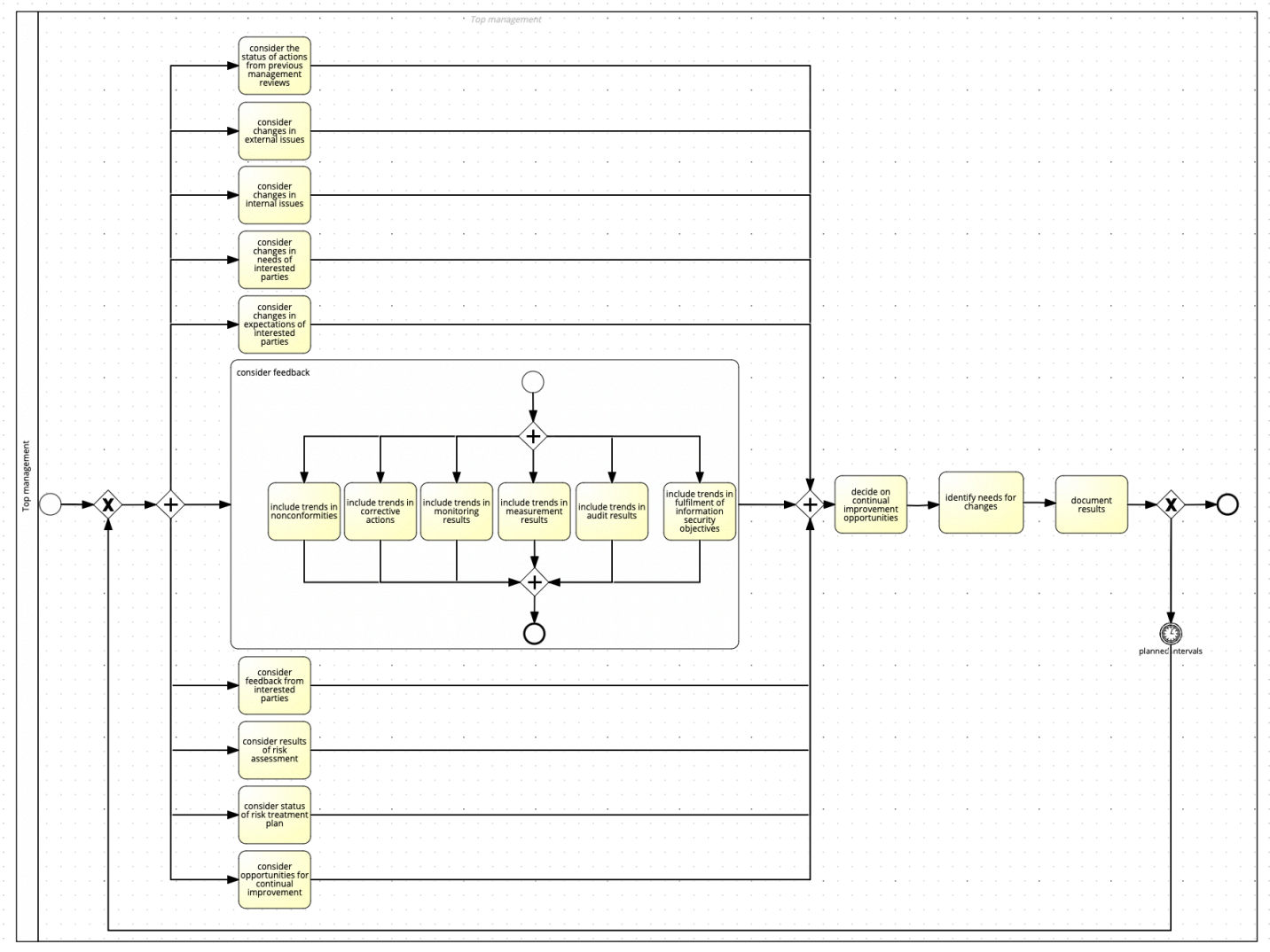
e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews."



3. GDPR

Text 8: Art. 33 GDPR Notification of a personal data breach to the supervisory authority

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. 2Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
1The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. 2That documentation shall enable the supervisory authority to verify compliance with this Article.

Text 9: Art. 6 GDPR Lawfulness of processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

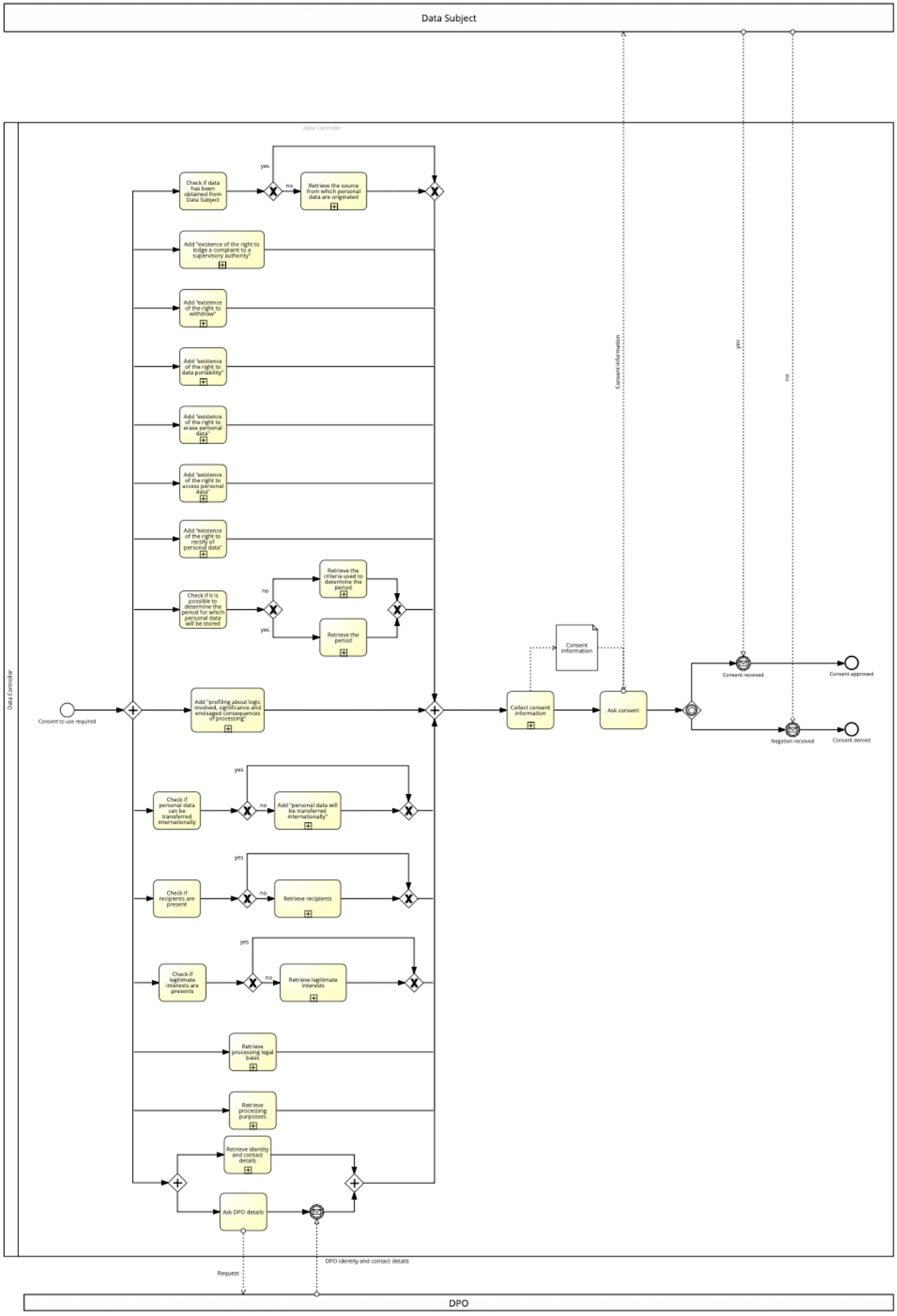
a) Union law; or
b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 3That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. 4The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d) the possible consequences of the intended further processing for data subjects;

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.



Text 10: Art. 15 GDPR Right of access by the data subject

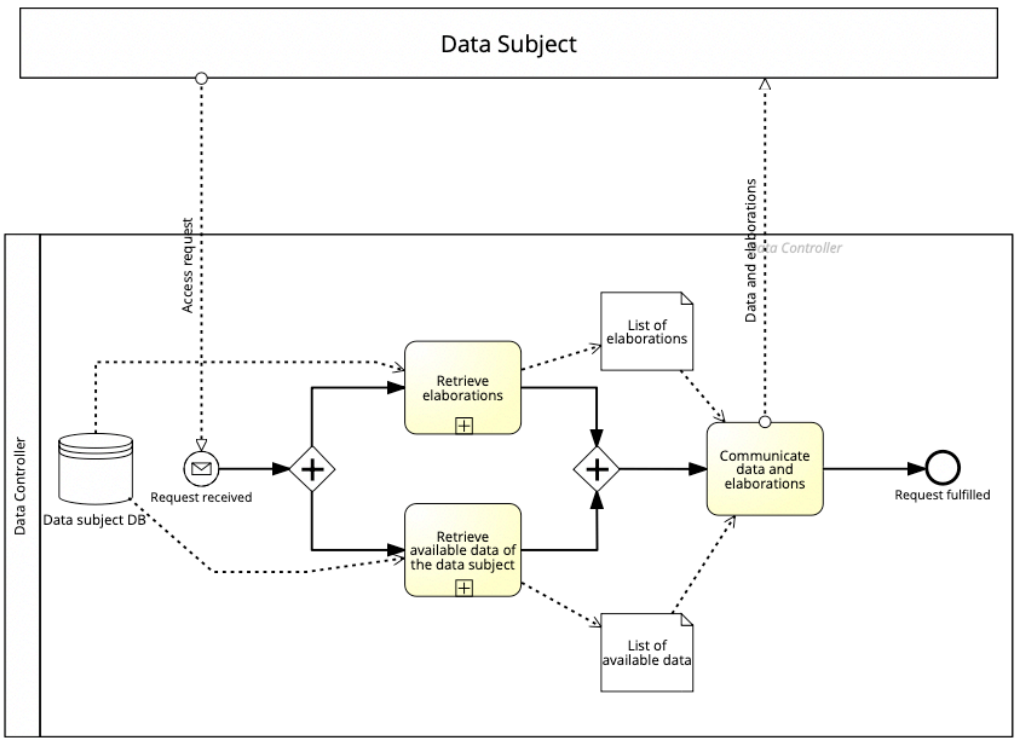
The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1. the purposes of the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
6. the right to lodge a complaint with a supervisory authority;
7. where the personal data are not collected from the data subject, any available information as to their source;
8. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

The controller shall provide a copy of the personal data undergoing processing. [2]For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. [3]Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.



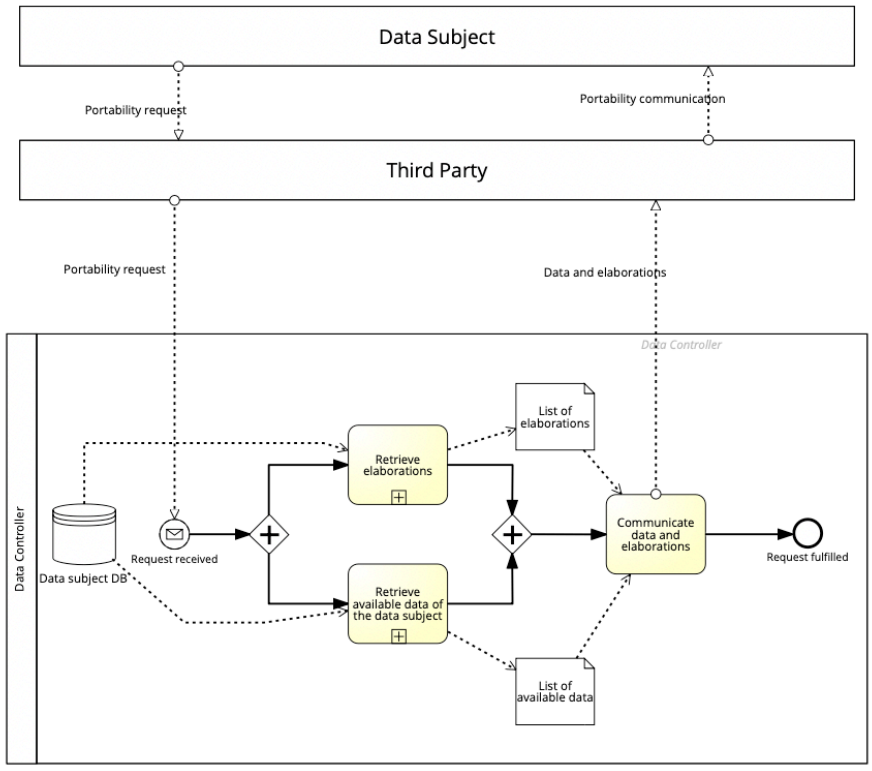
Text 11: Art. 20 GDPR Right to data portability

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.

In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.



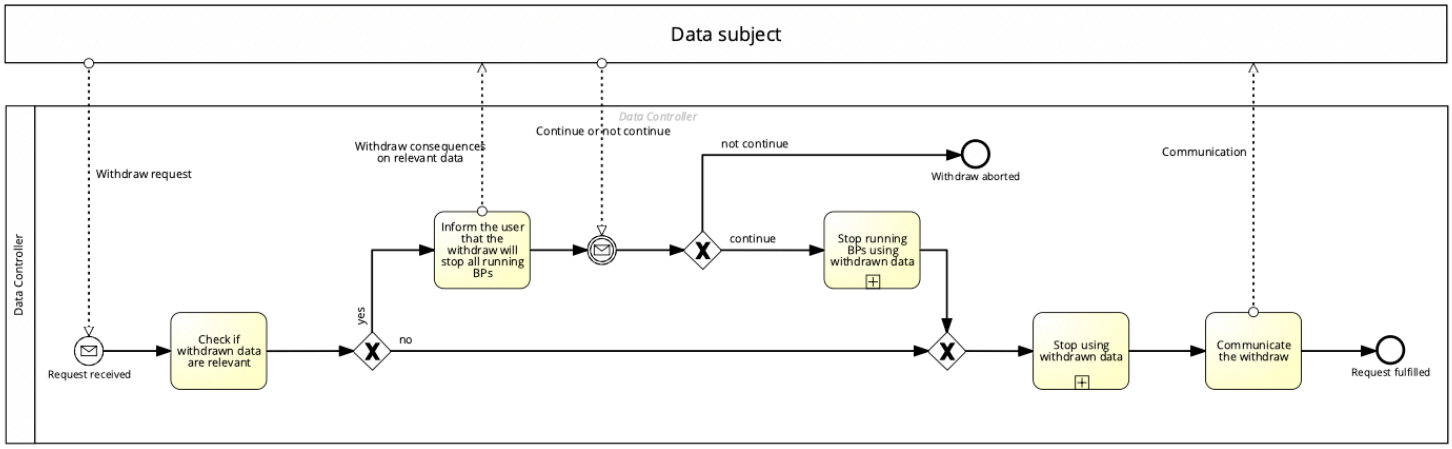
Text 12: Art. 7 GDPR Conditions for consent

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

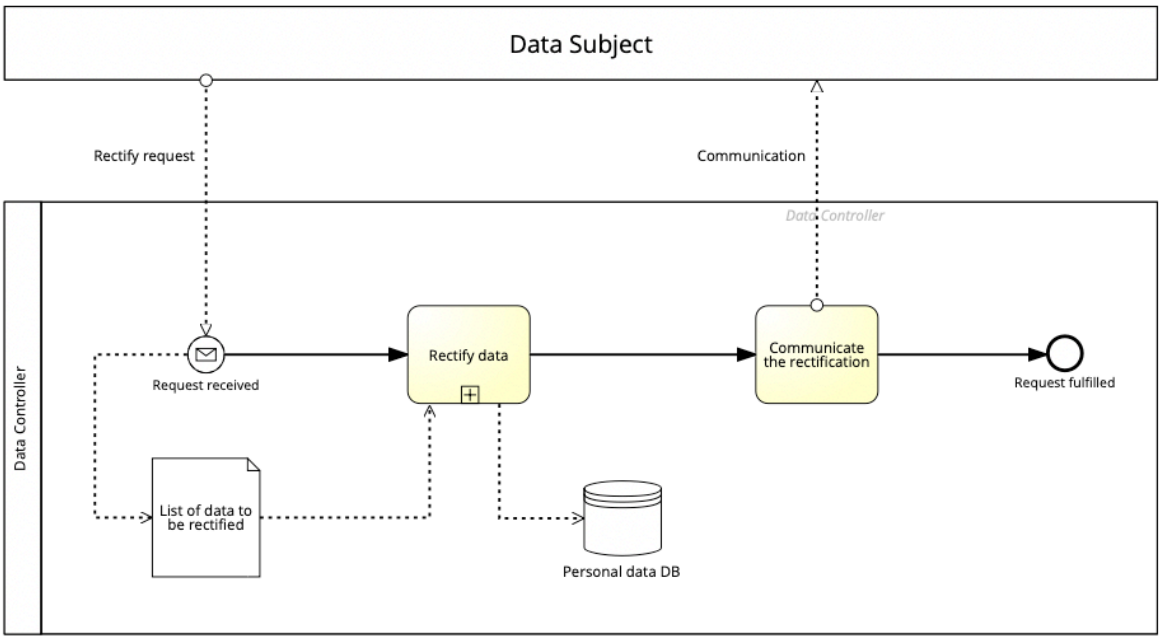


Text 13: gdpr_6_right_to_rectify → article 16 and 19 partly

article 16:
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

article 19, partly:
"The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16,"

Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.



Text 14: Art. 17 GDPR Right to erasure (‘right to be forgotten’)

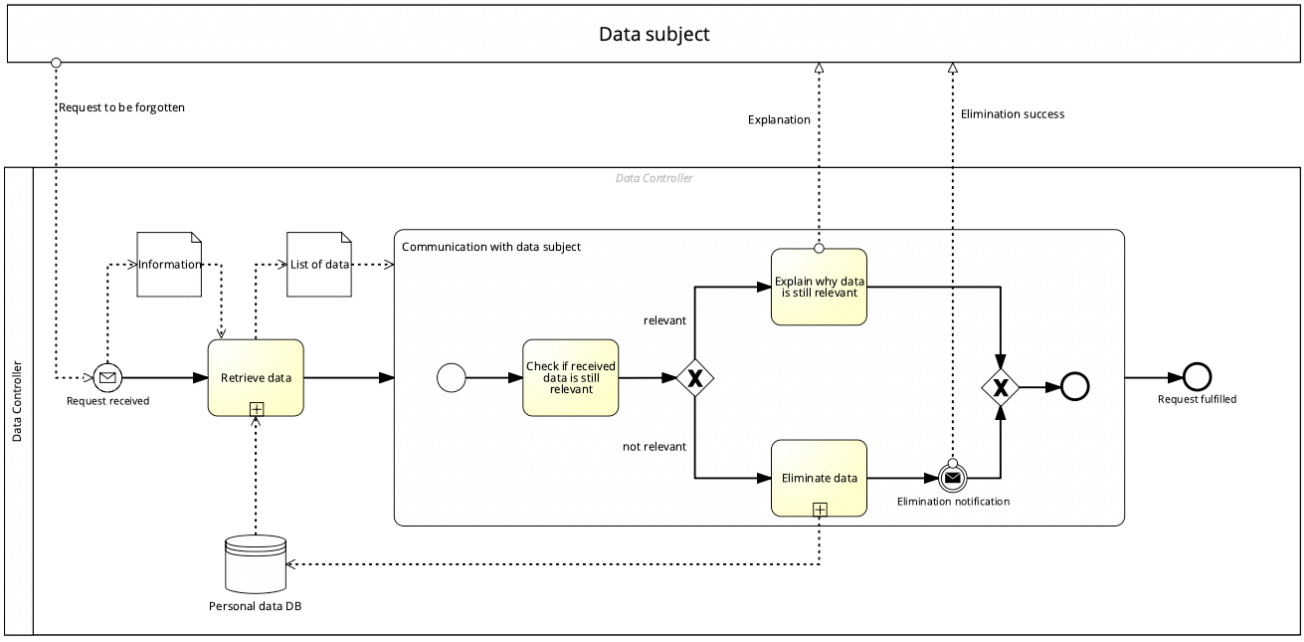
The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

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).

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

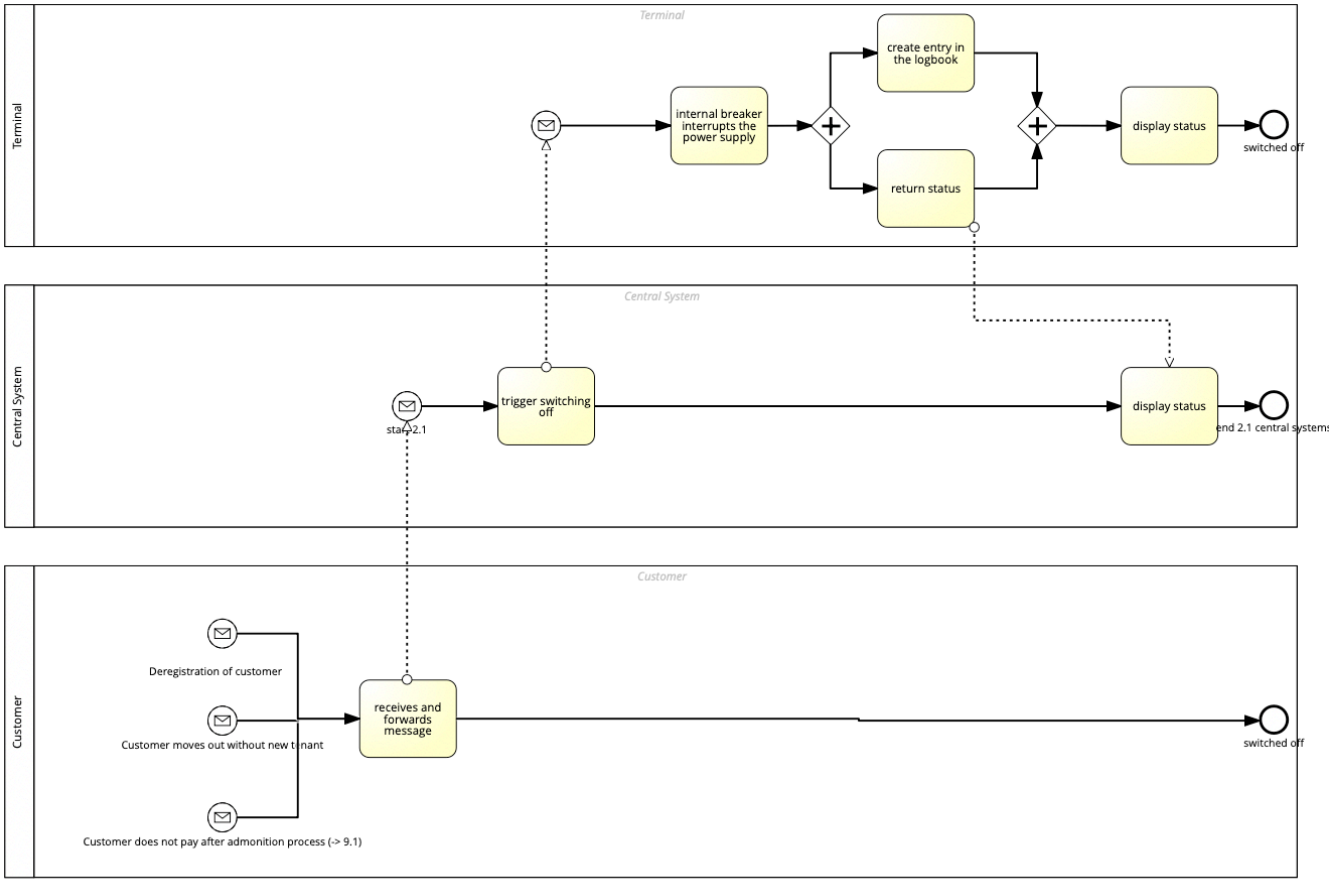
a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claims.



4. Smart Meter

Text 15: M2.1.bpmn → 2.1.txt

The aim is to remotely interrupt the supply of electrical energy for an object, as a result of a customer change or due to open collection claims, via the central system.
The shutdown takes place by opening the breaker present in the terminal.
From the central system, a shutdown command is transmitted to the affected terminal.
The terminal executes the received command, i.e., the internal breaker interrupts the power supply of the customer system, returns the status of the shutdown to the central system and creates an entry in the logbook.
This status must be visible on the terminal.
With collection there is no possibility of an immediate on-site reconnection by the customer after the blocking.
Input is either deregistration of current customer, customer moves out without new tenant or customer does not pay after admonition process.
The supply of electrical energy is interrupted, the status "interrupted" is displayed at the terminal and in the central system. An entry in the logbook of the terminal has been created.

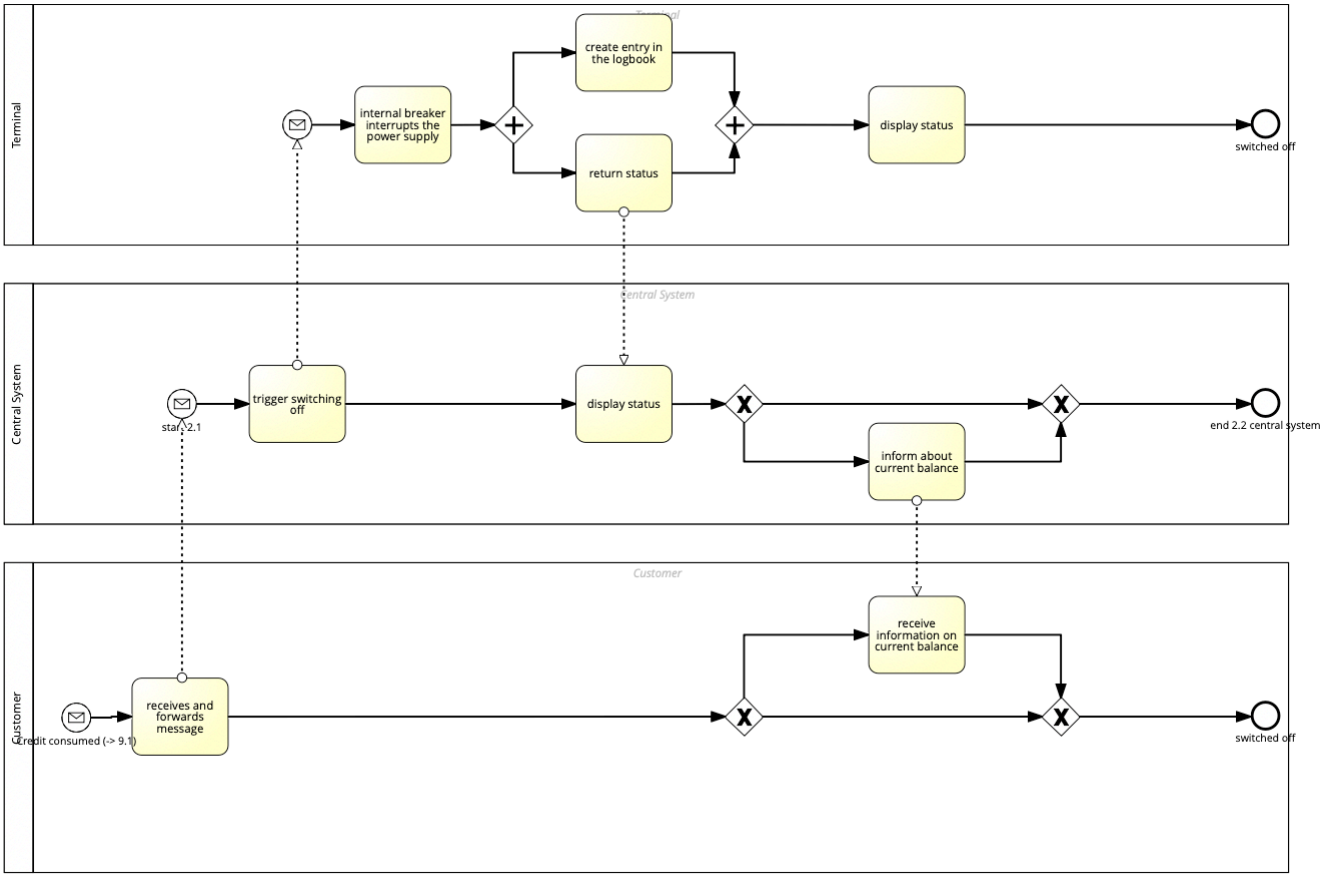


Text 16: 2.2→ 2.2

The prepayment function is realized via the central system.
The terminal only acts as a switching device.
The central system generates the shutdown command by comparing credits with consumption.
The comparison of credits with actual consumption value should be made periodically.
The basis is the daily readings.
A "real-time monitoring" is therefore not necessary.
Shutdown may only be carried out in compliance with legal conditions.
Each status change of the terminal must be displayed on the device and also create an entry in the logbook.
There may be a corresponding customer information about the current balance from the central system to the customer.

Credit or credit limit is consumed and shutdown time is within the legally allowed time window.

The supply of electrical energy is interrupted and the status of the breaker is displayed on the terminal, an entry in the logbook of the terminal is generated and the status is transmitted to the central system.

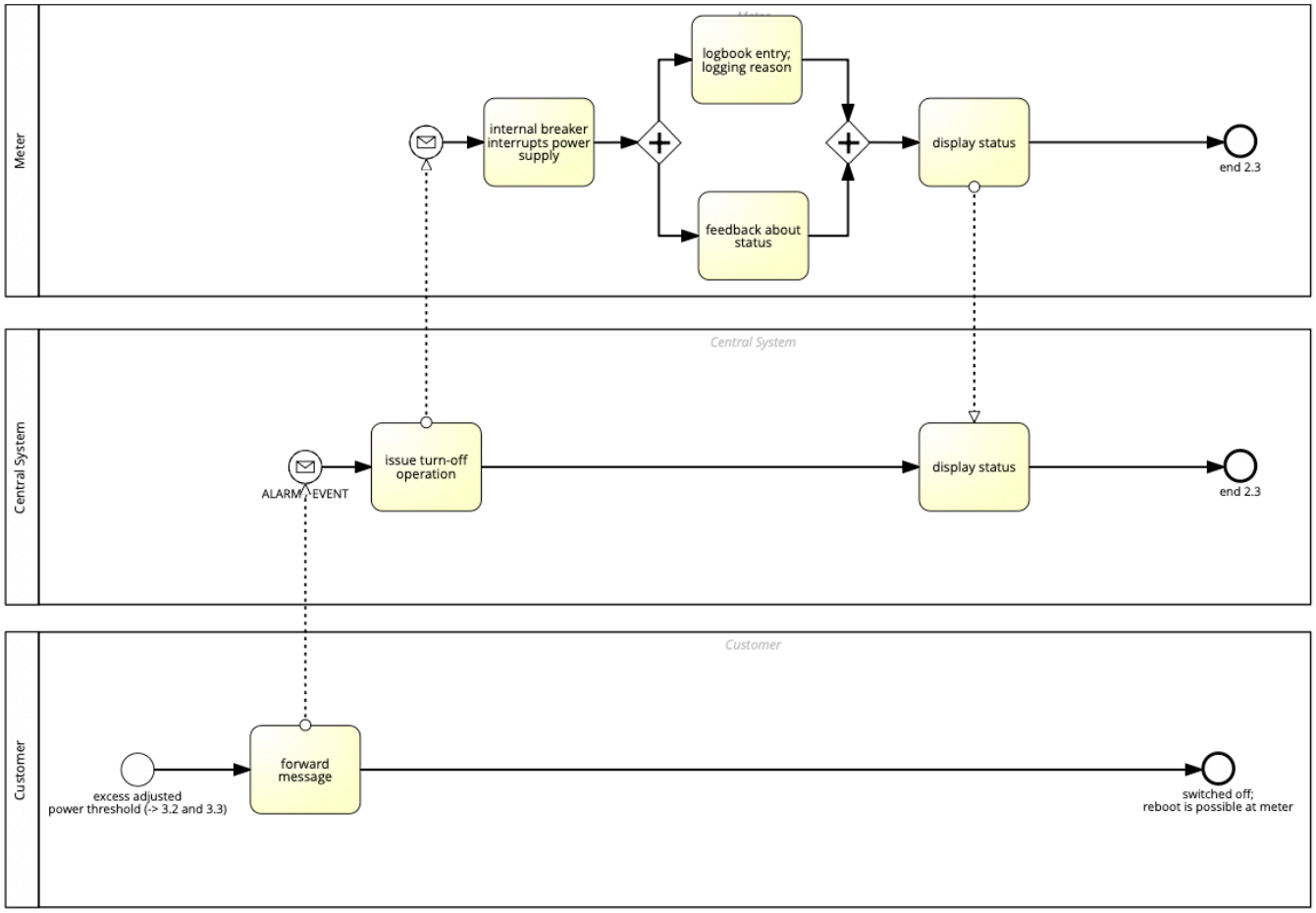


Text 17: 2.3 → 2.3

Exceeding an active power limit set in the meter and activated shuts down the customer system.
For the customer, immediate reclosing on site, ie directly at the meter, must be possible.
The shutdown, the message of the reclosing and the exceeding of the power threshold must be able to be transmitted to the central system as ALARM or EVENT and also visualized on the meter.
Breaker status is, e.g., OFF and READY.
An entry is also created in the logbook.
In the logbook, in addition to changing the breaker status, the reason for the shutdown, e.g. "Power limit exceeded by xxx watts" can be logged.

Exceeding the power threshold, for example in the context of the basic supply.

Exceeding the power threshold was entered in the logbook of the meter and transmitted to the central system as an ALARM or EVENT.

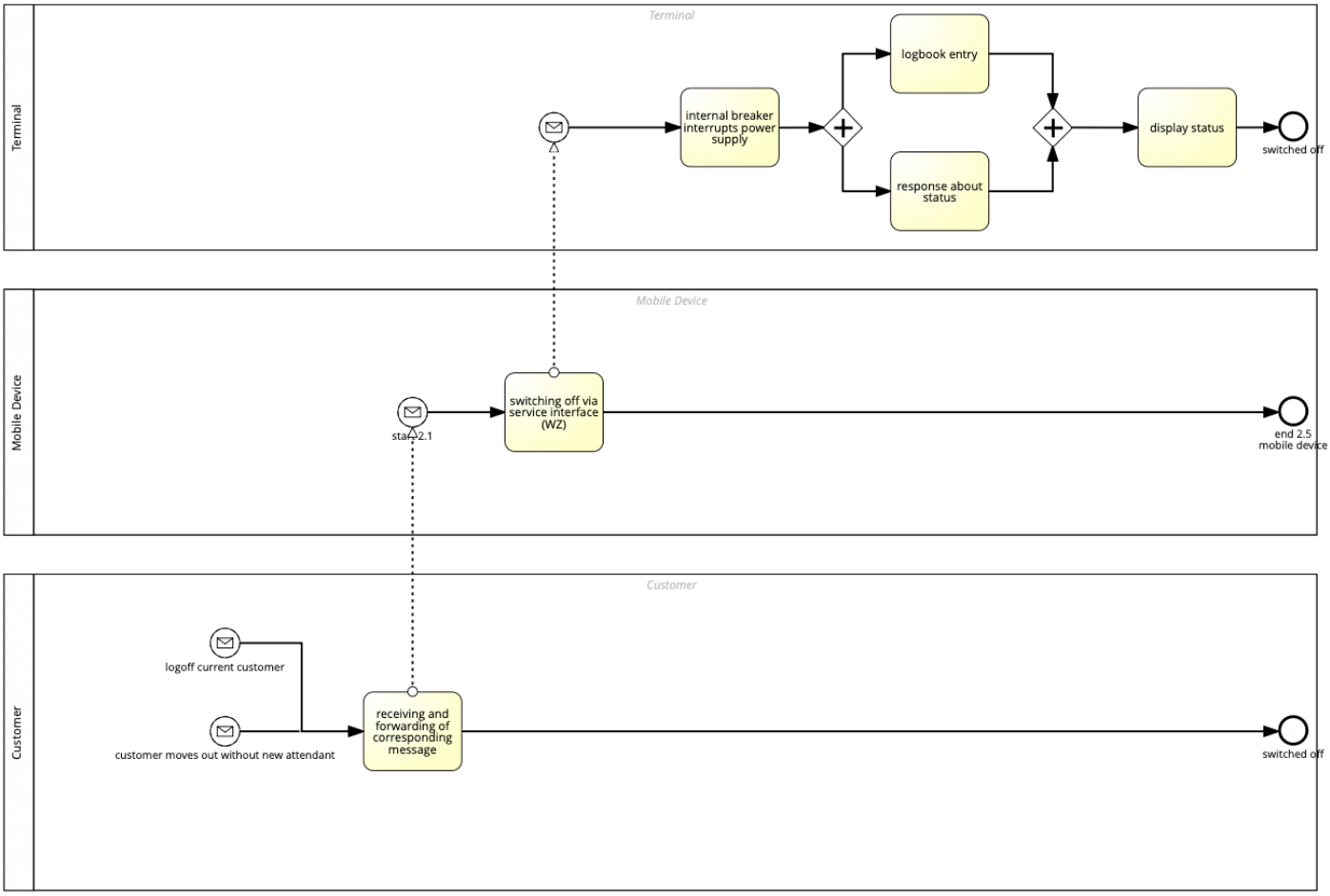


Text 18: 2.5

There is an elimination of the terminal on-site by means of a mobile device via the service interface (WZ). In order to meet the strict data protection regulations, the cryptographic parameters that authorize the device to be switched off must be stored on the mobile device.
It must therefore not be possible with these cryptographic parameters to turn off several or all terminals of the terminal equipment.
The cryptographic parameters must comply with the security concept from "OE Requirements Catalog End-to-End Security Smart Metering".

Input is either deregistration of current customer or customer moves out without new tenant.

The breaker of the terminal has switched off the system, indicating this on the device. An entry in the logbook of the terminal has been created.



Text 19: 3.1 / 3.3

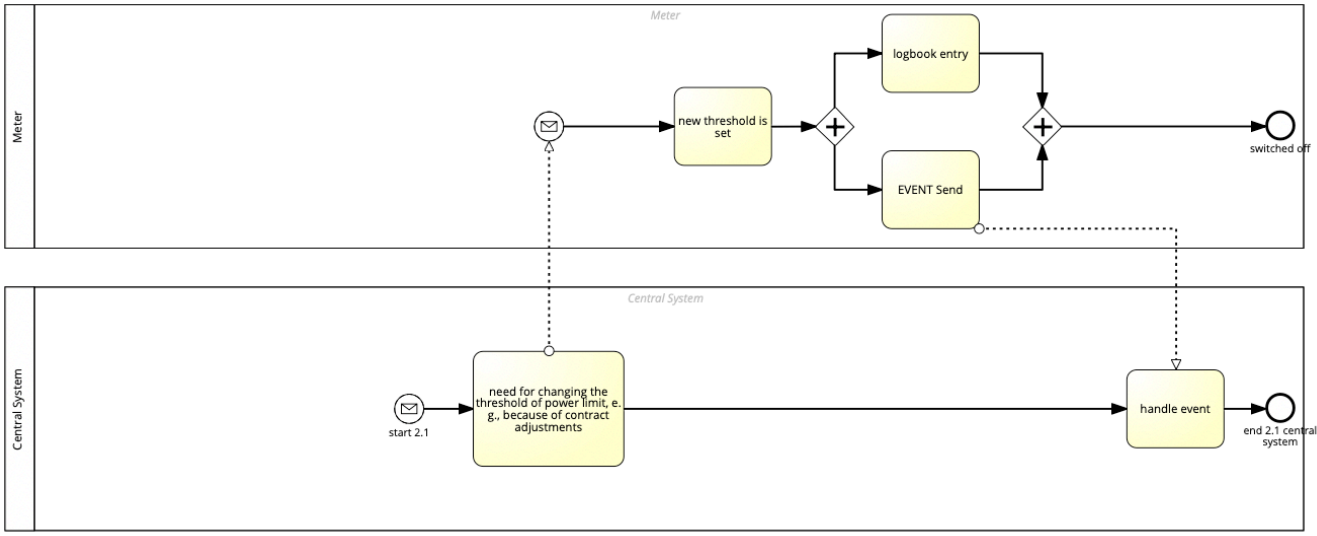
The operating limit of the meter is set by the control panel. Optionally this is possible for both energy directions.

Change requirement threshold of the power limitation, for example due to contract adjustments.

New threshold set, EVENT sent to the central system and logbook entry made on the meter.

The active power limit value of the meter must be able to be set locally via the service interface (WZ) of the meter. Optionally this is possible for both energy directions.

A logbook entry is generated. This state is transmitted to the central system as an ALARM or EVENT when the transmission link (WAN) is available.

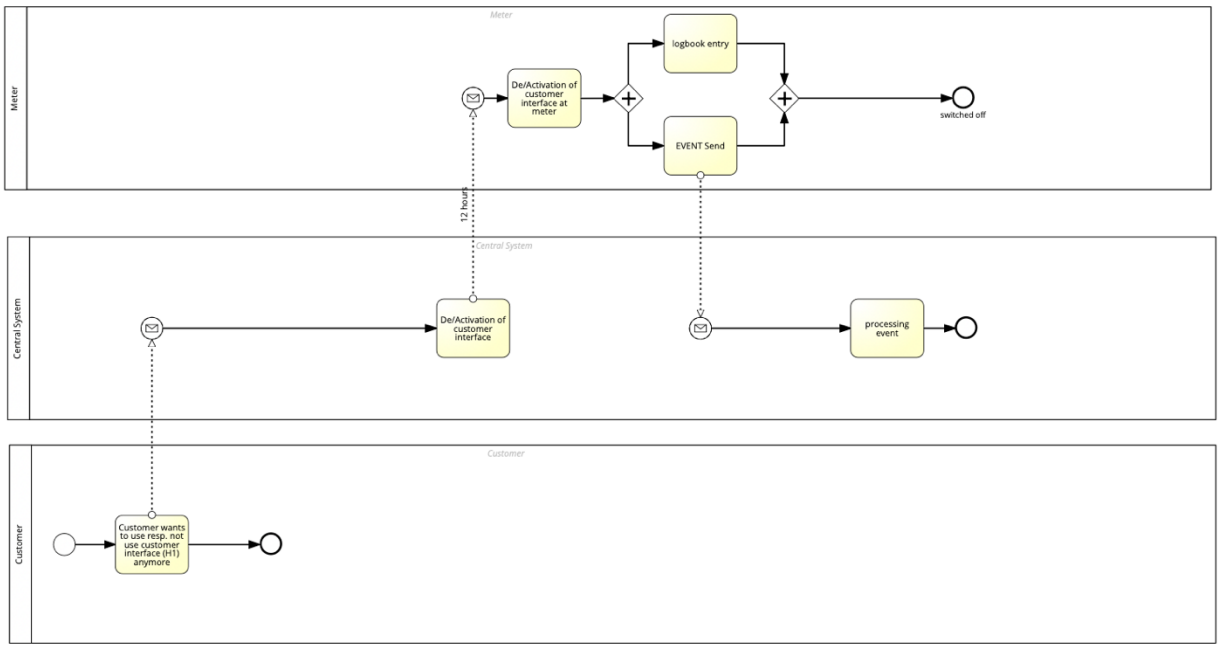


Text 20: 3.8

The customer interface (H1) on the meter is to be activated or deactivated from the central system, whereby it is deactivated by adefault. The control center receives an information status as ALARM or EVENT.

Customer wants to use or not use customer interface (H1) anymore.

Customer interface (H1) on the meter is activated / deactivated and there is an entry in the logbook. meter reports its status to the control panel as ALARM or EVENT.

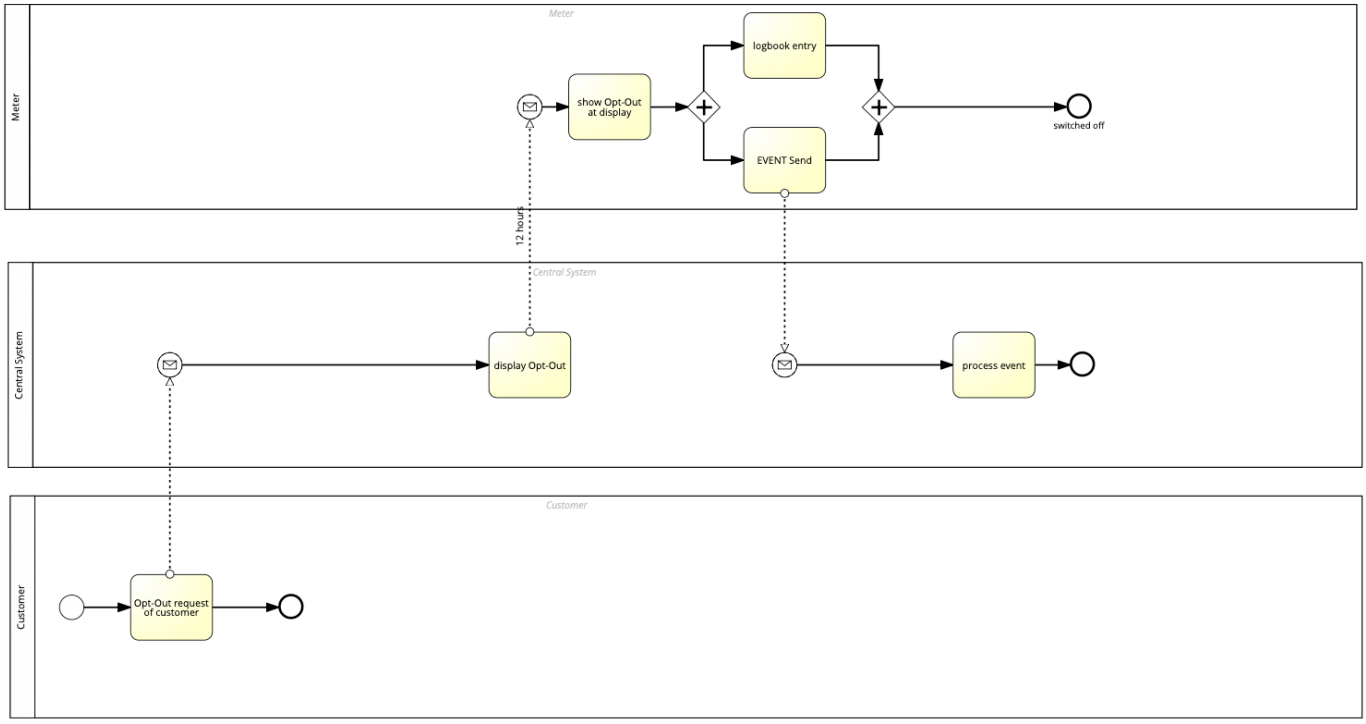


Text 21: 3.11

In the course of the so-called opt-out regulation, it must be possible for customers who refuse to install an intelligent electricity meter to deactivate the load profile recording in the meter. Activation / deactivation of load profile recording must be possible remotely (WAN interface). Each of these changes must be logged in the relevant legal logbook of the meter.
If the customer is opt-out, it must be displayed on the meter accordingly (for example, display, LED).

Opt-out request of the customer to implement at the NL.

Load profile recording is activated / deactivated and the information has been transmitted to the central system as ALARM or EVENT. A logbook entry has been made in the meter and the current status OPT-OUT is displayed on the meter.

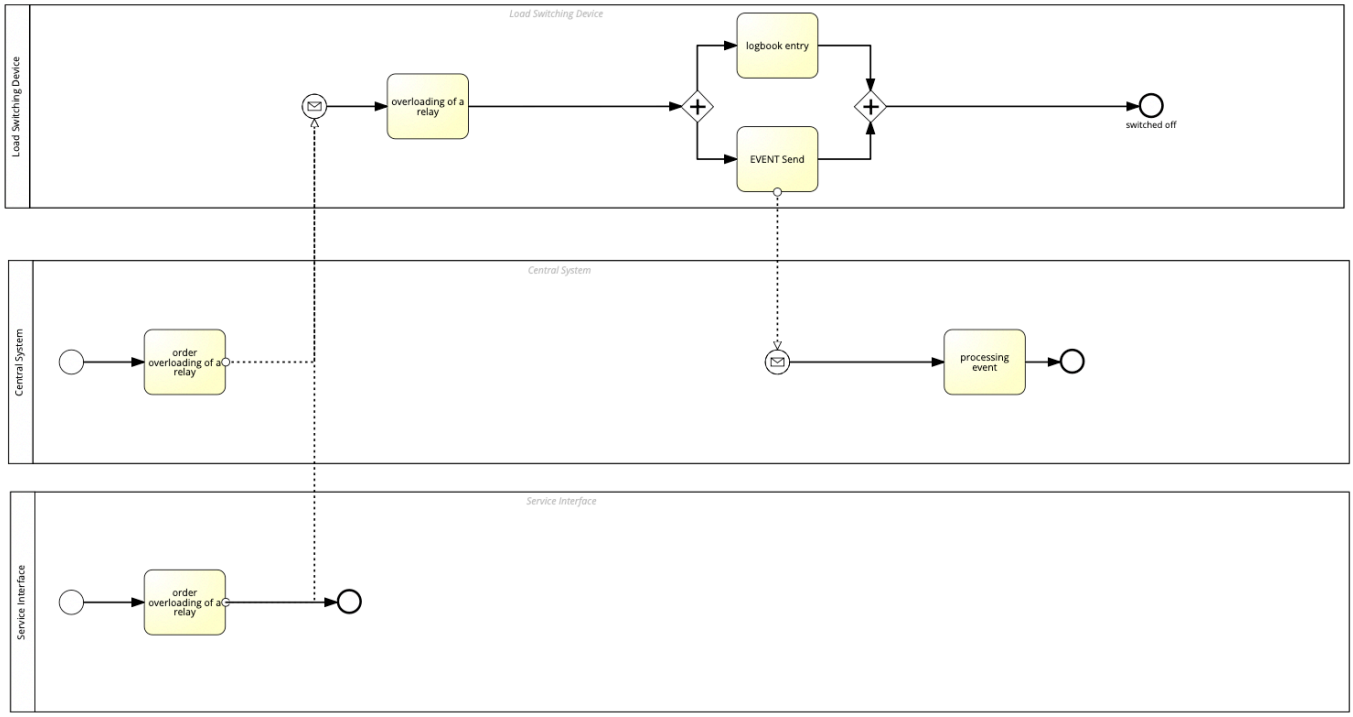


Text 22: 6.1

The load switching device is a completely independent of the meter device and serves as a possible replacement for a ripple control device or a timer. The load switching device has its own communication interface and can thus make contact with the control panel.
In principle, the relays follow a switching program specified by the central system and stored in the load switching device. However, it must be possible from the central system to override the circuit program with a spontaneous command (eg relay XY "OFF" or "ON"). The next opposite command (either from the switching table or from an external source) changes the state of the switching device.
The position of each relay or each switching cycle specified by the switching program must be reported back to the central system. The relay settings must also be visually displayed on site.

The central system sends a command to override a relay ("off" or "on"). The service interface is used to override a relay ("Off" or "On").

The corresponding relay in the load switching device switches to the desired status, reports this back to the central system and the position of the relay on the load switching device is also visible and a logbook entry is made.



Text 23: 6.3

For each relay in the load switching device, an independent, independent of the other relay switching program should be configurable. It should be possible to subdivide the circuit program into daily, weekly, seasonal and annual programs taking into account weekly, holiday and special days.

The switching program is managed centrally and transmitted to the load switching device via the communication paths. For control purposes, the circuit program must also be read-back. Any change to the circuit program, regardless of whether it is remotely executed, must be logged in a logbook.

The **central system** sends changed switching programs to the **load switching device**.

The load switching device receives the changed switching programs (feedback to the central system) and records this in the logbook.