The Relationship between Data Subject Rights

Bud P. Bruegger, ULD

1 Document Status

This is still a draft.

2 Acknowledgements

Help with many legal questions by Eva Schlehahn (ULD) is gratefully acknowledged.

The presented work was conducted as part of the SPECIAL project[1] that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 731601.

The visualizations were created using graphviz[2].

3 Purpose

The GDPR describes data subject rights in its Articles 12 through 23. The various paragraphs and letters within these articles often refer to each other. The objective of this paper is to visualize these relationships. For this purpose, the scenario illustrating the right to rectification is used.

Using the formalism of finite state machines[3], the paper intends to prepare for a possible later formalization of data subject rights in the ontology and vocabularies by the W3C's Data Privacy Vocabularies and Controls Community Group[4].

Beyond this, by presenting the subject matter in a technical (visual) language, it is hoped to provide support to technical professionals by fostering a better understanding of how data subject rights can be implemented in technical systems.

4 Basic Scenario

The following describes the basic scenario that provides the context for the discussion of this paper.

The paper assumes that there are multiple processing activities. In the foreground is the main processing activity conducted under the responsibility of *the controller*; in addition, there are multiple

[1] https://www.specialprivacy.eu/, last visited 24/10/2019.
[2] https://graphviz.org/
[3] See for example https://en.wikipedia.org/wiki/Finite-state_machine, last visited 24/10/2019.
[4] https://www.w3.org/community/dpvcg/, last visited 24/10/2019.

processing activities conducted under the responsibility of third-party *recipients* to whom the data collected by the controller have been passed on and thus disclosed. While these third-party recipients are controllers in their own right, they are usually called *recipients* in this paper to indicate their role in the scenario.

The scenario foresees that the data subject invokes one of her rights at the controller. While recipients need to grant data subject rights too, it is assumed that the data subject did not contact them.

To implement the processing activity, the controller uses both, employees and processors, who all operate under its direction. Employees and processors are considered to be recipients according to Article 4(9) since the personal data is disclosed to them. Third-party[5] recipients are external persons or entities to whom the personal data is disclosed by the controller, but who do not operate under its direction.

5 Technical Interpretation of the GDPR

This paper presents a technical interpretation of how the requirements of the GDPR can be implemented. One aspect of the interpretation is that it attempts to describe a good practice that may go beyond minimal requirements. Also the sequencing and grouping of the necessary actions are usually technically motivated.

It is assumed here that the processing activities by the controller and by the third-party recipients are geared towards maximal possible automation. Communications with the data subject are assumed to be made with electronic means and notifications of third-party recipients by the controller are assumed to be electronic and machine readable. While the technical interpretation given in this paper may also apply to scenarios with less automation, the sequencing and the grouping of actions may then have to be adapted accordingly.

An electronic implementation of data subject rights has several benefits, including ease of invocation on the part of data subjects, support of the controller to take actions without “undue delay” (see Article 12(3)), and limitation of the necessary work load on the part of the controller.

This paper is not concerned with discussing security measures, as for example those relative to authentication of data subjects, authenticity of notification messages, and confidentiality of communications in general. Readers who use this paper as guidance for their implementation are expected to take care of security aspects themselves in order to be compliant with the GDPR.

6 Technical Interpretation of Notification Obligations

The technical interpretation of the notification and information obligations of Article 19 deserves a more detailed discussion. In particular, the following first focuses on notifications of third-party recipients by the controller. It then also discusses information about notifications provided on request to data subjects.

[5] See Article 4(10) for the definition of “third party”

Article 19 mandates controllers to notify all recipients to whom personal data was disclosed about "any rectification or erasure of personal data or restriction of processing". "All recipients" encompass the controller's employees and processors, as well as all third-party recipients. Since we assume an automatic processing, we can assume that rectification, erasure, and restriction of processing, once actuated in the system, directly affect all employees and processors. This means that for these recipients, no specific notification is necessary. This means that only notification of third-party recipients are relevant to the discussion.

To understand the notification obligations, a closer look at why they are necessary is useful. Third-party recipients are controllers in their own right and therefore need to fulfill all obligations of the GDPR. This includes informing data subjects about their processing activities according to Article 14. It also includes the implementation of all data subject rights according to Articles 15 through 22. So why are the notification obligations necessary if data subject rights are already implemented by the third-party recipients?

To be able to exercise their rights, data subjects need to know about the processing, in this case that by the third-party recipient. The following looks at how such knowledge is created: On one hand, according to Article 14(3)(a), the data subject has to be informed "within a reasonable period after obtaining the personal data". This creates knowledge of the processing but is not guaranteed to happen immediately. On the other hand, the original controller needs to inform data subject about recipients. According to Articles 13(1)(e) and 15(1)(c), there is the possibility however, that only the categories of recipients are communicated. In that case, data subject don't even know about the recipients, let alone their processing activities. This means that even if controller and recipients comply with articles 13 through 15, there can be a time period in which data subjects lack the necessary knowledge to exercise their rights relative to processing by third-party recipients.

The notification obligations of Article 19 eliminate this risk by guaranteeing the "propagation" of data subject rights even to recipients who are yet unknown to the data subject. Considering that there can potentially be large numbers of third-party recipients, Article 19 also provides for a "single point of contact" for data subjects. This avoids preventing data subject rights through a potentially excessive effort necessary to contact all third-party recipients individually. Finally, should recipients fail to inform their data subjects as required[6], Article 19 prevents the possibility that they can hide behind unspecific "categories or recipients".

Technically, there are two distinct possible interpretations of the notification obligations of Article 19:

(i) The objective of the notifications is the synchronization of the data from the (authoritative) version kept by the controller with those versions kept by third-party recipients.
(ii) The objective of the notifications is solely the propagation of the invocations of rights by data subjects, leaving each party who keeps the data autonomous in their decisions.

This poses the question, which of these two interpretations applies.

[6] by article 14

On one hand, Article 19 requires the notification of rectification, erasure, and restriction, i.e., actions by the controller that affect the data. Technically, this seems to be consistent with (i). This is evident in the point in time of the notification being after the action was taken, i.e., potentially significantly after the point of time when the invocation of the right was received. Also, if the controller fails to take action[7], third-party controllers are not notified.

On the other hand, Article 19 fails to describe the action expected by recipients and thus relies on the Articles 5(1)(d) and 17(1) to regulate what recipients have to do. Consistently with this, the commentary of the GDPR by Simitis et. al[8] states that several constellations are possible where a recipient does not act on a notification. This seems consistent with interpretation (ii) since it leaves the decision of how to act on a notification to the recipient. In contrast, technical implementations of synchronization foresee "slaves" that copy the state of the "master" without questioning it.

If Simitis et al are right, technically this seems to speak for interpretation (ii) while the wording of Article 19 seems to imply interpretation (i). A technical implementation of Article 19 therefore cannot be undertaken without a certain flexibility in its interpretation.

The safest interpretation is probably to notify both, (ii) the reception of data subject right invocations (not required by Article 19), and (i) the corresponding actions taken by the controller (required by Article 19).

Further, while Article 19 only requires the notification of restriction of processing, it is technically evident that also the possible lifting of such restriction must be notified. Otherwise, from the point of view of recipients, restriction would be a terminal much rather than a temporary measure.

So far, the discussion has focused on notifications of third-party recipients. The following discusses the second part of Article 19 that requires to inform data subjects on request about such notifications. Here, from a technical point of view, the information provided to data subjects remains unsatisfactory. In particular, data subjects are only informed about notifications sent, not about actions taken by the recipients of these notifications. Since the third-party recipients do not receive an invocation of a right from the data subject directly, it remains unclear whether they have to provide information about actions taken[9]. The "single point of contact" in Article 19 is thus only a one-way concept of propagating invocations; it lacks the other direction which collects and informs about actions taken by recipients. The uncertainty about the requirements here can easily lead to situations where data subject cannot

[7] For example, a controller refrains from erasing data since it has another legal basis that permits further processing.

[8] Article 19, edge number 8, page 686 in Simitis / Hornung / Spiecker gen. Döhmann, Datenschutzrecht DSGVO mit BDSG Großkommentar, Herausgegeben von Prof. Dr. Dr. h.c. mult. Spiros Simitis, Prof. Dr. Gerrit Hornung, LL.M., Prof. Dr. Indra Spiecker gen. Döhmann, LL.M., 2019, 1474 S., Gebunden, ISBN 978-3-8487-3590-7

[9] It remains unclear, since Article 19 requires this solely of the controller who receives the request from the data subject.

detect when recipients simply ignore notifications. While this goes beyond the scope of this discussion, technical implementers are encouraged to consider providing a "two-way" single point of access.

The following concludes this section with an overall summary: A full technical interpretation of Article 19 should consider to:

- notify both, actions on the data taken by the controller (i above) and reception of invocations of data subject rights (ii above);
- not limit itself to a single step of disclosure to recipients, but support recursive notification to cover the case where recipients again have recipients;
- not limit itself to the direction of disclosure but also notify from a recipient back to the controller, for the case where data subjects invoke their rights by contacting a recipient much rather than the original controller;
- implement the concept of a single point of contact where
    - recipients inform data subjects about the single point of contact implemented by the original controller,
    - recipients also notify the actions they take in response to invocations of data subject rights back to the single point of contact,
    - the original controller implements a single point of contact where all relevant information is collected for the data subject. This could take the form of a dashboard. It could also facilitate data subjects to identify and contact recipients who fail to act on the invocation of rights.

The solutions shown in more detail in the diagrams below fall short of this, however, and, like Article 19, focuses solely on a single controller much rather than a complete multi-controller/recipient distributed system. This means that it fails to discuss how recipients shall react to received notifications. It also leaves away the consolidated status overview that a dashboard would provide about how third-party recipients handled data subject right invocations. The diagrams do however foresee the notification of both, the reception of invocations of data subject rights and actions affecting the data.

7 The Concepts of State Machines

State machines are used to model data subject right invocation and processing in this paper. This section briefly introduces the relevant concepts of state machines.

Finite-state machines are composed of a set of building blocks that are called *concepts* in the following. The most important concept is that of ***state***. Also fundamental is that of ***transition*** that permits the machine to change from one state to another. Transitions are triggered by ***events*** and enacted by ***actions***. While approaches such as UML state machines[10] differentiate between events and actions, this paper omits this distinction for simplicity.

[10] See for example https://en.wikipedia.org/wiki/UML_state_machine, last visited 24/10/2019.

Figure 1 shows a simple state machine. It is used to illustrate the symbols used to represent the various concepts. In particular, **states** are shown as **ellipses**. Optionally, states can make reference to an Article of the GDPR as is shown in *State B*. All concepts are numbered in parenthesis for easier reference from the describing text.

Changes from one state to another are called **transitions** that are depicted with **arrows** that connect states. Typically, transitions are governed by one or more **events/actions**. These express the event that triggers the transition or the action(s) that enact(s) the transition, respectively. Both, events and actions are represented by **boxes**. Events/Actions usually have an actor and may optionally reference an article of the GDPR.

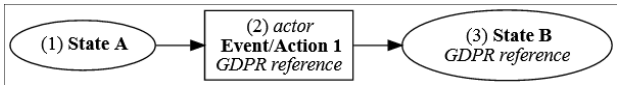


Figure 1: A simple example of a state machine.

Events and Actions in this paper correspond to a specific element of the GDPR. Compared to user interface events in technical implementations of data subject rights, the legal events are at times more detailed. For this reason, the visualization foresees the possibility of combining multiple legal events/actions into a single combined event/action of user interfaces. Such a combination is shown in Figure 2 where it is depicted by a dashed box.

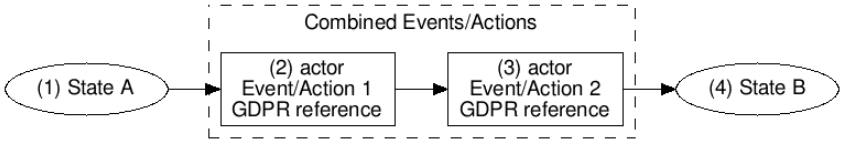


Figure 2: Combination of multiple events/actions.

At times, the transition between states depends on the outcome of an action. In other words, the "flow" branches. This is depicted in Figure 3 by using a rhombus symbol.

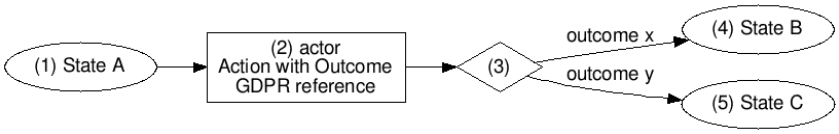


Figure 3: Branching of the transition flow.

8 States of Processing in the GDPR

This section describes the different states of processing used in this paper. The GDPR introduces one of these states explicitly, while another two are implicit. The following first discusses restricted processing, the state explicitly named in the GDPR and then discusses the implied states.

8.1 Restricted Processing

In Article 18, the GDPR introduces the concept of "**restriction of processing**" or "**restricted processing**" (in this text, these two terms are used as synonyms). What restricted processing means is laid out in paragraph 18(2). In particular, it states that "Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or [..]".

The fact that it is an individual data subjects to obtain restriction of processing (see 18(1)) clarifies that the restriction regards one or several data records belonging to a single data subject. When a data subject has obtained restriction, her data records can still be stored by the controller, but cannot be processed in any other way, unless specific conditions--such as consent by the data subject--are met. The GDPR uses the words "with the exception of storage" since in the GDPR, also storage is considered a form of processing (see Article 4(2)).

Expressed in a language more familiar to computer scientist, restriction of processing means that the data records belonging to a given data subject could for example be marked as restricted; then, processes that typically operate on data regarding a multitude of data subjects have to filter their input such that any data records marked as restricted are excluded. An alternative implementation could be to temporarily move the restricted data to another processing system[11].

8.2 Implicit States of Processing

The existence of the state of "restricted processing" implies two other states.

Since a restriction is imposed on processing under certain circumstances, there obviously also exists an "**unrestricted processing**". In other words, restricted processing implies another state of processing that we will simply call "***normal processing***".

The restriction of processing in the GDPR is of **temporary** character. This is for example evident in the fact that a restriction can be lifted (see Article 18(3) GDPR). This temporary character of restriction implies that there must also be the possibility of a permanent or terminal restriction of processing. We call this implied state of simply "***terminated processing***". Note that, following the principle of storage limitation (see Article 5(e) GDPR, terminated processing usually goes along with the deletion of the affected data records.

In summary, the three states of processing that are taken into account in this paper are:

- **Normal processing**,
- **restricted processing**, and
- **terminated processing**.

[11] See Recital 67 GDPR on methods by which to restrict the processing of personal data.

9 Transitions between States of Processing

With the states of processing defined, we are interested in transitions between these states. Figure 4 shows the theoretically possible transitions. More interesting are the details of these transitions, however, in particular, transitions caused by the invocation and processing of data subject rights according to the GDPR. This is the topic of the remainder of this paper.

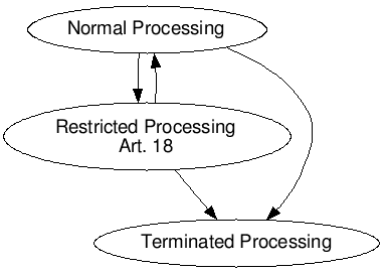


Figure 4: Possible transitions between states of.

10 The Right to Rectification

This subsection discusses state transitions in relation to the right of rectification according to Article 16 GDPR. The details of the state transitions are illustrated in Figure 5. The following text describes and discusses the figure in more detail.

(xx The figure is at the moment inserted at the end in a temporary version xx)

The state transition diagram starts in a state of normal processing [1]. The main trigger for the described transitions is the invocation of the right to rectification by a data subject according to Article 16 (see action [3]). The need for such rectification can be recognized by the data subject either (i) due to a change in the real world (e.g., a change of residence or phone number) that needs to be reflected in the data, or (ii) after inspecting the data and detect an inaccuracy. In the latter case, it is often a pre-requisite to a request of rectification that the data subject can access the data stored by the controller according to Article 15. Such access is depicted in the action [2].

Arguably, it would be unfair on the part of a controller to further process a person's data unchanged even after receiving a request for rectification. For this reason, in Article 18(1)(a), the GDPR foresees that in this particular situation, processing can be restricted. Since the GDPR states that the "data subject has the right to obtain" such restriction, the option is left open that the data subject refrains from making use of this right. To eliminate such uncertainty, it may be safer for the data subject to explicitly request such restriction. This is illustrated in action [4].

Since the requests of rectification and restriction of processing are given at the same point of time, they are shown as a combined (user interface) event (see dashed box).

This single user interface event optionally also contains a third request: The data subject has to decide whether to make use of another right that is described in the second sentence of Article 19 GDPR. This article is concerned with the situation where the personal data were already passed on to third-party

recipients[12]. In this case, it is obviously necessary to pass on invocations of data subject rights (see section 6 above). According to Article 19, this information only has to be provided "if the data subject requests it." This is thus a choice of the data subject. Action [5] shows the case where the data subject decided to invoke this right. It is important to note that in our case, Article 19 refers to two distinct data subject rights, namely that invoked in Action [3] and that invoked in Action [4]. Accordingly, as indicated in Action [5], information is requested about both, rectification and restriction.

On receipt of the data subject's request [4], the controller needs to restrict processing. This is represented by the new state [6] of "restricted processing" in in Figure 5. It is assumed here that the technical mechanism used for imposing this restriction prevents all internal recipients of the data (i.e., employees of the controller) and all possible processors from further processing the concerned data. This is relevant since it means that the technical mechanism of restriction can be considered a communication of the restriction to all internal recipients and processors according to Article 19.

With these recipients already notified, this leaves only third-party recipients to be notified. This notification is executed in Action [7]. In addition to the notification of the invocation of the right to restriction in Action [4], it propagates also that of rectification of Action [3]. For the latter case, it must also include the rectified data provided by the data subject in [3]. Note that this notification of the invocation of rights was recommended in Section 6 above although it is not explicitly requested in Article 19.

Since requested by Action [5], the controller must now inform the data subject of these notifications. This is done in Action [8]. It is noteworthy that here, the controller needs to inform the data subject about each single recipient to whom the rectification request was communicated. This contrasts with the option to inform data subject solely about the categories of recipients, as stated in Articles 13(1)(e) and 14(1)(e), respectively.

The controller now needs to verify the accuracy of the personal data referred to by the request (action [9]). It may not always be possible to fully automate this action. As indicated in Article 18(1)(a), the GDPR assumes that verification takes time. This can also be the case even if the verification can be fully automated. Consider for example that the contested data is an e-mail address and that the controller uses an automatic e-mail verification procedure that sends a one-time code to the indicated address. In this case, the duration of the verification depends on how rapidly the data subjects acts on the verification e-mail.

Verification determines whether the data provided by the data subject are indeed factual. This can have two possible outcomes, as is illustrated in the branching [10]. For example, the e-mail verification can provide evidence that the provide e-mail address is indeed controlled by the data subject or not.

In the case of acceptance of the rectification (left branch), the controller now needs to apply the rectification to the data (Action [11]). Again, we assume that the now rectified data are automatically

[12] See Articles 4(9) and 4(10) GDPR for the definition of third-party recipient.

visible to all employees and processors. This satisfies the notification requirements of Article 19 for all but third-party recipients. The latter are therefore notified in Action [12]. Note that the notification now concerns the change of data by the controller. In contrast to the invocation of rights, this notification is actually mandatory according to Article 19.

Since the requested rectification has now been executed in Action [11], and the restriction of processing was solely motivated by the inaccuracy of the data (Article 18(1)(a)), no more reason to further maintain the restriction persists. The controller can therefore lift the restriction of processing by transitioning back to the state of normal processing ([30]). Before this is possible, several requirements of notification and information have to be satisfied, however.

In a first step, it is technically sound to notify third-party recipients that the preciously communicated restriction has now been lifted. This is achieved in Action [13] that is sent as combined communication together with the notification of Action [12]. Note that this is not directly required by the GDPR but is necessary according to the technical interpretation of Article 19 in Section 6 above.

In addition, various pieces of information have to be communicated to the data subject. This can be seen as the response to the request that comprises Actions [3] through [5]. The most important information is probably that the requested rectification was executed. This is represented by Action [14] and based on Article 12(3). Further, Article 19 explicitly requires that (if requested in Action [5]) the data subject is informed about the recipients of notifications in Action [12]. According to Article 18(3), it is necessary to inform the data subject about the upcoming lifting of the restriction. This is done in Action [15]. If requested by the data subject in action [5], with Action [16], the controller also provides information about the notifications about the lifting sent to third-party recipients in Action [13]). Again, this is not explicitly requested by Article 19 but recommended by its technical interpretation in Section 6.

With all these obligations fulfilled, the controller can now continue with normal processing [50]. This completes the right branch where the rectification request is accepted by the controller.

The remainder of this section describes the right branch after [10] where the controller rejected the rectification based on a negative verification of the data-subject-supplied data in Action [9].

In accordance with Article 12(4), the controller needs to inform the data subject about the rejection and its reasons. It also has to inform about the possibility of lodging a complaint with a supervisory authority[13] and seeking a judicial remedy. This is done in Action [21]. In the according communication, the controller asks the data subject to choose how to proceed. There are the following options:

(i) The data subject accepts the rational for rejection and gives consent to lift the restriction and continue with normal processing.
(ii) The data subject corrects the submitted data for a renewed verification by the controller
(iii) The data subject invokes the right to erasure according to Article 17.

[13] It is good practice to provide contact details for the supervisory authority.

At least in the case where the verification in Action [9] wasn't instantaneous, the controller now has to wait for a reply. This is represented by state [22]. Even if the information to the data subject in Action [21] was sent by e-mail, it should be possible to collect the response by the data subject online. For this purpose, the e-mail could for example contain a one-time URL to an input form.

The state of waiting can be left if one of Actions [23] through [26] trigger transitions. These are discussed in sequence in the following.

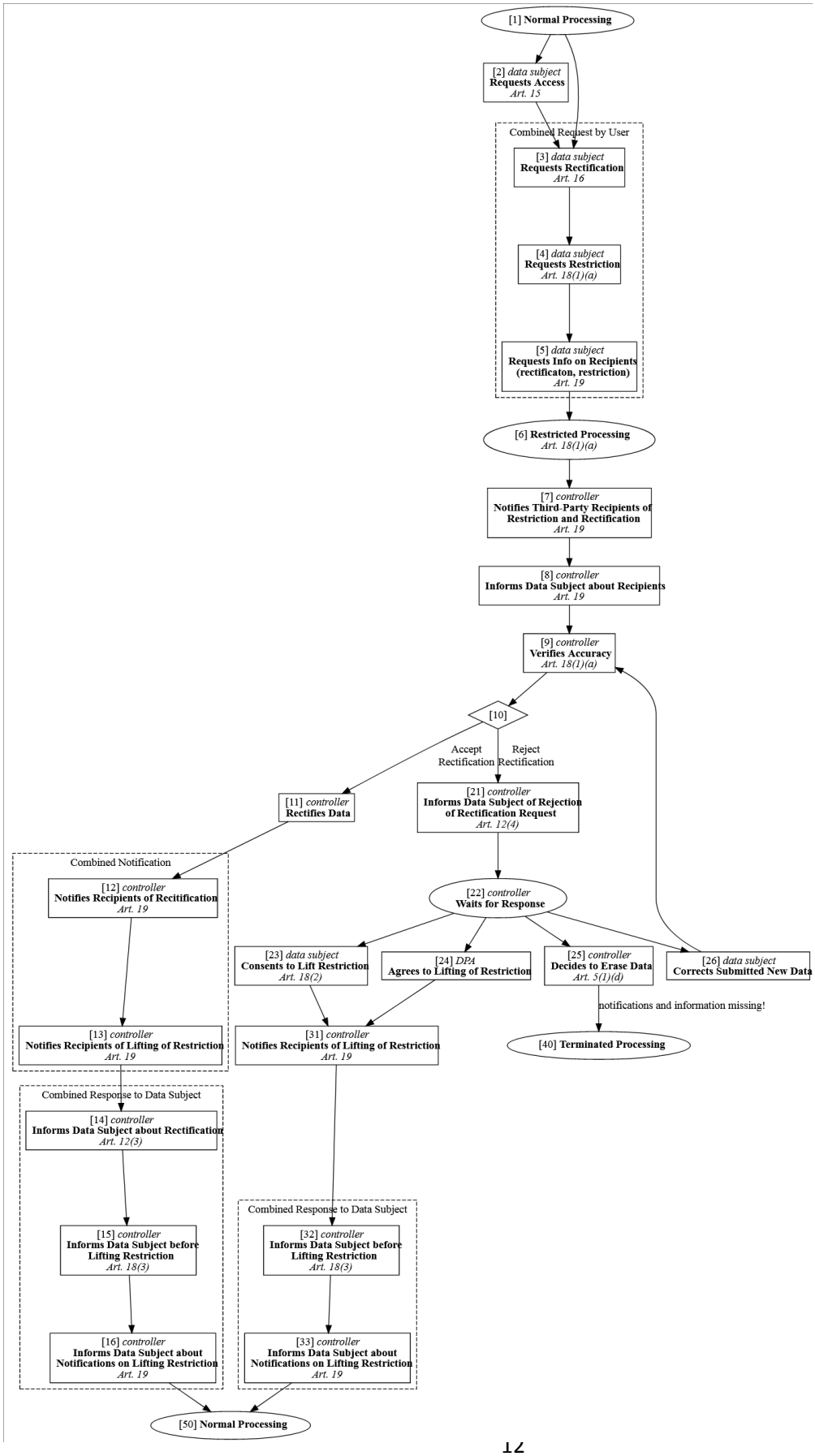
In Action [23], the data subject accepts the reason for rejection of the rectification request and gives consent to lift the restriction and continue with normal processing. This consent is one of the possible reasons given in Article 18(2) that a restriction can be lifted.

In Action [24], it is assumed that the data subject lodged complaint with a supervisory authority and that the controller gets to know that the authority approves the lifting of the restriction and continuation of normal processing.

In these two cases ([23] and [24]) the restriction can be lifted after the necessary notifications and information to the data subject. These closely resemble those already discussed previously.

In Action [25], the controller decides unilaterally to not wait any longer and instead erase the restricted data and terminate processing concerning this data subject. This is based on Article 5(1)(d) that states *erasure* as one possible option for controllers to handle inaccurate data. After the necessary notifications and information of the data subject, the processing can then be terminated [40].

In Action [26], the data subject believes that the verification by the controller in Action [9] failed due to an error in the newly provided data. The data subject then provides a corrected version of this data for renewed verification. This loops back to Action [9].


[1] Normal Processing
[2] data subject
Requests Access
Art. 15
Combined Request by User
[3] data subject
Requests Rectification
Art. 16
[4] data subject
Requests Restriction
Art. 18(1)(a)
[5] data subject
Requests Info on Recipients (rectificaton, restriction)
Art. 19
[6] Restricted Processing
Art. 18(1)(a)
[7] controller
Notifies Third-Party Recipients of Restriction and Rectification
Art. 19
[8] controller
Informs Data Subject about Recipients
Art. 19
[9] controller
Verifies Accuracy
Art. 18(1)(a)
[10]
Accept Rectification
Reject Rectification
[11] controller
Rectifies Data
[21] controller
Informs Data Subject of Rejection of Rectification Request
Art. 12(4)
Combined Notification
[12] controller
Notifies Recipients of Recitification
Art. 19
[22] controller
Waits for Response
[23] data subject
Consents to Lift Restriction
Art. 18(2)
[24] DPA
Agrees to Lifting of Restriction
[25] controller
Decides to Erase Data
Art. 5(1)(d)
[26] data subject
Corrects Submitted New Data
notifications and information missing!
[13] controller
Notifies Recipients of Lifting of Restriction
Art. 19
[31] controller
Notifies Recipients of Lifting of Restriction
Art. 19
[40] Terminated Processing
Combined Response to Data Subject
[14] controller
Informs Data Subject about Rectification
Art. 12(3)
Combined Response to Data Subject
[15] controller
Informs Data Subject before Lifting Restriction
Art. 18(3)
[32] controller
Informs Data Subject before Lifting Restriction
Art. 18(3)
[16] controller
Informs Data Subject about Notifications on Lifting Restriction
Art. 19
[33] controller
Informs Data Subject about Notifications on Lifting Restriction
Art. 19
[50] Normal Processing