Explanatory notes to the processing of the comments received during the consultation of the draft versions of the *2014 ACM Procedure for the inspection of digital data* and *2014 ACM Procedure regarding the legal professional privilege of lawyers*

In this document, the Netherlands Authority for Consumers and Markets (hereafter: *"ACM"*) explains how it processed the comments received from market participants during the consultation of the draft versions of the *2014 ACM Procedure for the inspection of digital data* and *2014 ACM Procedure regarding the legal professional privilege of lawyers* (hereafter jointly to be referred to as: *"the Procedures"*). The comments of the market participants have been included in this document (in Dutch, see *annex*).

1. Background

On April 1, 2013, the Establishment Act of the Netherlands Authority for Consumers and Markets came into force.[1] From that date, ACM has been the legal successor to the Netherlands Consumer Authority (hereafter: CA), the Netherlands Competition Authority (hereafter: NMa), and the Netherlands Independent Post and Telecommunications Authority (hereafter: OPTA). As a result of its establishment, ACM sought to create uniform procedures for inspecting digital data, as well as regarding the legal professional privilege of lawyers. The best practices of the CA, the NMa and OPTA have been used as a basis. The Procedures replace the procedures that were used by the CA, the NMa and OPTA prior to the merger.

On July 3, 2013, the Procedures were submitted to market participants for consultation. In addition, a consultation meeting took place on July 16, 2013. In that meeting, ACM gave a more detailed explanation, and market participants were given the opportunity to react directly to the draft versions. A significant number of parties attended the consultation meeting, and submitted a verbal reaction. In addition, ACM received written reactions to its draft versions from the following seven market participants: DLA Piper Netherlands, Loyens & Loeff, the Advisory Committee on Competition Law of the Dutch Bar Association, Stibbe, the Association for Competition Law (hereafter: VvM), CMS and TenneT TSO B.V.. These written reactions have been included in the *annex* to this document. ACM is grateful to all market participants that

---

[1] Establishment Act of the Netherlands Authority for Consumers and Markets (*Dutch Bulletin of Acts* 2013, 102).

have given a reaction for their comments as these comments enable ACM to improve on the draft versions of the Procedures prior to the finalization thereof.

2. Processing method of received reactions

2.1 General

ACM has received and processed a large number of useful suggestions from market participants. The way many of these points have been processed does not require further explanation. These suggestions concern, for example, improvements to the text of the Procedures (such as making the definitions clearer) or removing omissions in the draft versions of the Procedures (such as the moment of handing over the objective and subject of the investigation).

However, several points from the reactions are discussed below. For these points, it is desirable to explain in greater detail their processing method or the decision not to process them.

2.2 2014 ACM Procedure for the inspection of digital data

Safeguards or process description

Various market participants indicated that including a process description offers transparency in the process in each case. The *2014 ACM Procedure for the inspection of digital data* does not contain a process description as such, but ACM, by offering safeguards, outlines the framework within which ACM exercises its powers, and explains how individuals involved are able to verify that exercise. The rationale behind this choice is the desire for creating a single procedure that is applied by all of ACM's departments. With a process description, such a uniform application is not possible because ACM's procedure varies depending on, among other aspects, the type of regulation that is enforced. This was explained in greater detail during the consultation.

Nevertheless, ACM considers transparency for market participants of the utmost importance. ACM is therefore fully aware of the importance of providing further information about the procedure that is applied in cases. ACM will thus offer the individual involved further information about the procedure preceding the application of the *2014 ACM Procedure for the inspection of digital data* and *2014 ACM Procedure regarding the legal professional privilege of lawyers*.

Inscope software equipped with search function

ACM uses special software (*InScope)* to facilitate claims filed by individuals involved. ACM has updated this software following the reactions of market participants by adding a new viewer

technology. Users (businesses and law firms) have explicitly called on ACM to add search functionality. At first, ACM did not wish to respond to these calls because the responsibility for the correctness of the process of claiming data (or parts thereof) as 'privileged' or as 'non-business' lies with users, and specifically not with ACM. With the addition of a search function in the Inscope software, it could be argued that ACM must take full responsibility for any missed files when searching. Even though ACM still does not wish to nor is even able to influence the way such claims are made, ACM has changed its position. ACM thus wants to meet the explicit and widely-shared wish that was expressed during the consultation. ACM has added a functionality in Inscope that helps users find privileged and/or non-business data in the relevant data set. Users will have to active this functionality first in order to be able to use it. With this activation, users assume responsibility for the search results. With these improvements, ACM wishes to make it easier for users to file claims on time.

Deadlines

Various market participants have indicated that they would like to see deadlines be included in the *2014 ACM Procedure for the inspection of digital data* for filing claims. ACM believes that fixed deadlines are not in line with the idea behind this procedure (see above section 'Safeguards or process description'). What exactly a reasonable deadline is, differs per situation. For example, the size and structure of the data set, among other factors, affect the deadline. That is why ACM did not meet this wish of several market participants, and why no deadlines have been included. ACM will set an appropriate, reasonable deadline on a case-by-case basis. Users will always have the opportunity to file a request for extending deadlines, supported with reasons.

Moment of making available for perusal

VvM noted that the rights of the defense would be harmed if the moment of perusal of the search query list were different from the moment that was set in the *NMa's Procedure in relation to the Inspection and Copying of Analog and Digital Data and Documents*. It has been laid down in the *2014 ACM Procedure for the inspection of digital data* that perusal is granted at the moment the statement of objections is made available for perusal. The reason behind this choice is the fact that ACM carries out different types of investigations, which require different procedures. In general, a search query list in an investigation into compliance with the Dutch Competition Act is finalized sooner than a search query list in an investigation into compliance with Section 11.7, paragraphs 1 through 4 of the Dutch Telecommunication Act (the 'spam prohibition'), because the former is usually the result of a continuous process whereas the latter is the result of an iterative process. In the *2014 ACM Procedure for the inspection of digital data*, it is laid down that ACM aims to make the search query list available to the individuals

involved as soon as possible. It is expected that, in practice, this will hardly be any different from the previous procedure used in antitrust investigations.

Capacity of 'individuals involved'

When the Procedures were drawn up, the question arose about which of the parties involved in the investigation should the rights of verification be awarded to. At the consultation meeting, ACM specifically asked the attendees to react to this question. It has been laid down in the Procedures that the rights of verification are, in principle, awarded to the addressee when investigative powers are exercised. The reason behind this choice is that, among other reasons, the addressee has the obligation to cooperate as laid down in Section 5:20 of the Dutch General Administrative Law Act (hereafter: Awb) when investigative powers are exercised. This obligation to cooperate is applicable within the scope of ACM's powers. The safeguards included in the Procedures limit these powers. The rights of verification of compliance with these safeguards should therefore be granted to the addressee of the powers. Although ACM will use the foregoing as its starting point, the principle of proportionality laid down in Section 5:13 of the Awb may lead, under certain circumstances, to the designation of a different (or another) market participant as 'individual involved'. The above line of reasoning is consistent with ACM's approach in its assessments of data confidentiality. It should be noted in that context that compliance with the safeguards is ACM's own responsibility, irrespective of the question of whether or not an individual involved verifies if ACM does so.

Judicial authorization in advance

VvM noted that it remains to be seen whether the lack of judicial authorization in advance in case of dawn raids can be reconciled with Article 8 of the European Convention on Human Rights (the right to privacy). According to ACM, the General Court recently answered this question affirmatively[2].

Additional safeguards in case of searches of homes

VvM additionally noted that the *2014 ACM Procedure for the inspection of digital data* do not provide any additional safeguards in case of investigations conducted on the premises of private individuals' homes. ACM is of the opinion that, in this regard, the *2014 ACM Procedure for the inspection of digital data* can be reconciled with European law since investigations conducted on the premises of private individuals' homes are only carried out with judicial authorization in advance, in which case the proportionality of ACM's actions is assessed.

---

[2] General Court 6 September 2013, joined cases T-289/11, T-290/11 and T-521/11.

Investigations conducted on-site or at the offices of ACM

The *2014 ACM Procedure for the inspection of digital data* has been phrased in such a way that the exact location of the investigation (securing data, and conducting data searches) is not explicitly described. Based on previous experiences, ACM's basic rule is that securing data takes place on-site, and that data searches are conducted at the offices of ACM. However, circumstances in individual cases may result in departures from the main rule. Various market participants have indicated that they consider the dawn raid's site the primary location for conducting data searches. ACM did not adopt this point. Data is secured on-site. Depending on the nature and magnitude of the data, as well as technical capabilities, ACM decides where the data search will be conducted. In most cases, this will be done at the offices of ACM. Considering technological developments and public acceptance of digital communication in general, the amount of data that is found at businesses will only increase even further. In order to come to specific data sets, it is currently common practice to search using search queries. With regard to the choice of whether data processing occurs on-site or at the offices of ACM, several aspects are important such as the structure and size of the data set, but also current technological capabilities of forensic investigation (for example, the extent to which data must be processed in a forensic investigative manner before they can be filtered). ACM aims to produce as small as possible 'within-scope data sets'. What is certain is that the more specific the final investigation data set becomes, the less likely it is that this can be carried out on-site within a reasonable amount of time (proportionality). The current situation, in which ACM increasingly wishes to generate specific investigation data sets, means that ACM will, in general, carry out data processing at the offices of ACM (main rule). In each case, ACM will be as transparent as possible in advance about the procedure it will follow, and about the location where these activities will take place.

Being present when the within-scope data set is created

Referring to the court ruling in the Fortis-Allianz[3] case, market participants have indicated that they should be present when ACM investigates the secured data set. ACM is of the opinion that individuals involved must be given the opportunity to be present when ACM investigates the secured data set if data are inspected during such investigations. If ACM carries out a search query on the secured data set, ACM will only perform actions that do not require data to be persued. The reason that ACM performs such actions without market participants being present, regardless of the question of where the search query takes place, is two-fold. First, there are practical reasons. These actions usually take up a lot of time, and may even last several days. In addition, it is usually not possible to make an accurate estimate of how long

---

[3] Court of The Hague (Vzr,) 13 October 2008, CLI:NL:RBSGR:2008:BH2647, *Allianz/ State of the Netherlands.*

these actions will take. Second, from an investigative perspective, ACM does not wish to provide market participants unlimited insight into its forensic investigative capabilities and strategies. However, the latter does not take away the fact that, in its forensic investigations, ACM observes the safeguards as laid down in the *2014 ACM Procedure for the inspection of digital data,* and that individuals involved will be given the opportunity to verify ACM's compliance with these safeguards, which is also provided for in this procedure. Furthermore, it must be noted that being present when these actions are performed would not offer the individuals involved any insight into the data in question. After securing the data (creation of the secured data set), a number of forensic IT steps follow such as 'unpacking' emails, preparing certain files so they can be searched, and filtering system data. ACM uses different tools in these steps, during which no data can be inspected. The actual search is a technical step using software with which no data can be inspected either.

The foregoing does not take away the fact that an individual involved can be invited to be present when the secured data set is investigated if ACM is planning to peruse data before any within-scope data set has been created yet. Individuals involved are expected to take a seat in a separate room for the inspection. Individuals involved must be able to contact the enforcement official directly if there is any reason to do so. The reason behind ACM's request to have individuals involved take a seat in a separate room is that, most of the time, the data must be processed in a lab environment, where officials can work on multiple cases simultaneously or on data from multiple undertakings. In addition, the enforcement officials must be able to consult with each other without an individual involved being present. For these reasons it is undesirable to have an individual involved directly present.

Within-scope data set is not proportional

Two market participants have indicated that the procedure with searches lead to non-proportional data sets because only the result of a selection would be the determining factor for proportionality. Since the *NMa's Procedure in relation to the Inspection and Copying of Analog and Digital Data and Documents*[4]*,* the NMa has held the opinion that the data that belong to the scope of the subject and objective of the investigation are determined using a selection based on search queries that are directly related to the subject of objective of the investigation. If a certain file is selected using one of these search queries, it falls within the within-scope data set. Individuals involved have had and continue to have the opportunity to react in response to the search queries that are handed over, after which an adjustment of the search queries could/can

---

[4] Of 20 August 2010. This procedure (in Dutch) can be found on https://www.acm.nl/nl/publicaties/publicatie/4747/NMa-publiceert-werkwijze-analoog-en-digitaal-rechercheren/.

take place if they, on second thought and in that specific case, appears to be not appropriate and/or not specific enough. In this procedure, the selection method is the determining factor, and not just the result, for the proportionality of the investigation. In the *2014 ACM Procedure for the inspection of digital data,* the same approach to this particular point has been taken as in the procedures that had been used since 2007 by the NMa. According to ACM, this approach is prompted by the circumstances of digital data investigations.

Handing over the secured data set to the individual involved

As previously mentioned, ACM selects data on the network of the individual involved and then secures the data on-site. The selected data of the individual involved that are secured (the source data), are thus, in principle, located at the individual involved himself, and not at ACM. When securing data, ACM recommends the individual involved to make a copy of this data set on its own network, and to save this copy. ACM does not make a separate copy for the individual involved. ACM uses hash values of the secured data set to be able to verify that this data set is identical to the selected source data. The hash values are handed over to the individual involved. At the end of a dawn raid, ACM hands over to the individual involved a list of files and their hash values. It is thus clear what files belong to the secured data set, and that they are a correct copy of the source data. The individual involved himself has the source data. ACM therefore does not hand over to the individual involved a copy of the secured data set.

Retention periods of data sets

Following the reactions with regard to the retention periods of data, ACM considered returning the secured data set to the individual involved once ACM has drawn up the statement of objections in the investigation in question. However, the reason for storing the secured data set at ACM is two-fold: being able to conduct a new search, and proving that a certain file really comes from the individual involved. More specifically, ACM considered whether a secured data set can be returned to an individual involved if he declares that all files in the investigation data set, the within-scope data set and/or the secured data set indeed come from him. The moment that was chosen in this hypothetical situation was the moment ACM had drawn up a statement of objections in the investigation in question, because, at that point, no searches would be necessary anymore (the first above-mentioned purpose for storing the secured data set). In the end, ACM chose not to include such a provision in the *2014 ACM Procedure for the inspection of digital data*. This is because, once a statement of objections has been drawn up, ACM's Legal Department or the courts could then order an additional investigation. For carrying out searches in such additional investigations, it is thus necessary to have the secured data set (second purpose).

To clarify the retention period of data sets, ACM included the definition of completions of investigations in the *2014 ACM Procedure for the inspection of digital data.*

2.3 2014 ACM Procedure regarding the legal professional privilege of lawyers

Status of employed lawyers

One reaction to the *2014 ACM Procedure regarding the legal professional privilege of lawyers* revealed that it was unclear whether correspondence between an individual involved and an employed lawyer was also privileged. The explanatory notes have been adjusted accordingly to clarify that this is the case.

More detailed interpretation of the term 'cursory look'

Several reactions to the *2014 ACM Procedure regarding the legal professional privilege of lawyers* revealed that it was insufficiently clear what was understood by the term 'cursory look'. The explanatory notes to the procedure provide a more detailed interpretation of the term 'superficial inspection'.[5]

The term 'to make a plausible case'

Following the reactions it received, ACM chose to provide a more detailed interpretation of the term 'to make a plausible case' in Article 3, paragraph 4 of the *2014 ACM Procedure regarding the legal professional privilege of lawyers.*[6]

Independence of the LPP officer

In various reactions to the *2014 ACM Procedure regarding the legal professional privilege of lawyers*, it was noted that the independence of the LPP officer was not safeguarded, whereas he operates under the responsibility of ACM. In the explanatory notes, ACM clarified that, although an ACM LPP officer, given his official employment with ACM, is not completely independent of ACM, he has been given explicit instructions to carry out his duties independently of officials that are charged with carrying out the investigation. It has been additionally clarified that the choice for the procedure in which the LPP officer makes an assessment is a voluntary choice.

---

[5] In line with General Court 17 September 2007, joined cases T-125/03 and T-253/03 (*Akzo Nobel Chemicals and Akcros Chemicals/Commission*), paragraph 81.

[6] In line with General Court 17 September 2007, joined cases T-125/03 and T-253/03 (*Akzo Nobel Chemicals and Akcros Chemicals/Commission*), paragraphs 81 and 82

Waiting period

In several reactions to the *2014 ACM Procedure regarding the legal professional privilege of lawyers*, it was noted that the waiting period of five working days for seeking legal remedies would be unfeasible in practice. In the *2014 ACM Procedure regarding the legal professional privilege of lawyers*, ACM extended the waiting period to 10 working days.