EUROPEAN DATA PROTECTION SUPERVISOR

Prior checking Opinion on the reception of notifications and exchange of information between the Agency for the Cooperation of Energy Regulators (ACER) and national regulatory authorities

Brussels, 02 October 2015 (2015-0545 and 2015-0657)

1. Proceedings

On 26 of June 2015, the European Data Protection Supervisor (EDPS) received a notification for prior checking from the Data Protection Officer (DPO) of the Agency for the Cooperation of Energy Regulators (ACER) relating to the exchange of information between the Agency and national regulatory authorities ("NRAs") relating to potential breaches of Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency ("REMIT") through the Case Management Tool (the "CMT") Furthermore, on 10 of August 2015 the EDPS received another notification from ACER on the reception of notifications relating to potential breaches of REMIT through the Notification Platform (the "NP"). In the present Opinion, the EDPS has decided to examine jointly the notifications due to their close relationship.

According to Article 27(4) of Regulation 45/2001 (the Regulation) this Opinion must be delivered within a period of two months, not counting suspensions for requests for further information[1], in other words, by 5 October 2015.

2. The Facts

CMT is ACER's tool for cooperating with national regulatory authorities (NRAs) in the framework of its tasks under Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT).[2] The NP is a tool for submitting notifications to ACER and NRAs, both of suspected breaches and for exemptions/delays provided for in REMIT.

ACER, in collaboration with NRAs, monitors the trading activities in wholesale energy products to detect and prevent insider trading and market manipulation. At national level, NRAs are entrusted with investigatory and enforcement powers against suspected market abuse. Breaches of REMIT are liable to penalties which can be either administrative or criminal depending on national procedural arrangements. ACER shall ensure coordination and consistency in the application of REMIT by NRAs at national level.

[1] Questions were raised on 10 July, 4 August 2015 and 14 August 2015, to which ACER replied on 20 July 2015, 10 August 2015 and 25 August 2015. The draft Opinion was sent to ACER for comments on 21 September 2015; comments were received on 1 October 2015.
[2] OJ L 326/1, 08/12/2011

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.eu.int - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

The REMIT Regulation establishes various cooperation obligations between ACER, NRAs and other actors. Among others, NRAs shall, without delay, inform ACER where they have reasonable grounds to suspect that acts in breach of REMIT are being, or have been, carried out in a Member State. Where ACER has such information, it may ask NRAs to start investigations. ACER may also receive notifications of suspected breaches of REMIT from informants in the general public. Finally, ACER may also establish and coordinate investigatory groups with NRAs for cross-border cases. ACER does not have investigatory powers of its own and will carry out administrative and coordination tasks for the investigatory groups.

The NP is a web application through which the NRAs, competent financial authorities of the Member States (CFAs), market participants (MPs) and persons professionally arranging transactions (PPATs) can notify incidents to ACER and NRAs. The information received through the NP might trigger the opening of a case in CMT but ACER and NRAs may receive notifications through other channels as well. The NP is also used for notifications from MPs willing to benefit from the exemptions/delays[3] provided for in REMIT,.

There are different categories of data subjects in the NP and CMT:

1. Staff members of NRAs and ACER;
2. Persons submitting notifications;
3. Persons involved in/associated with a possible breach.

The data categories differ between the categories of data subjects. For category one, basically professional contact details will be processed; for category two, contact information including the role of the notifying party and information on the suspected breach; for category three, contact details (where available) and information on the suspected breach.

ACER has prepared two separate privacy statements for CMT and two separate privacy statement for the NP. One each is aimed at category one data subjects and is provided upon activation of the user account in the NP and CMT. The other one aimed at categories two and three. It will only be provided to category two data subjects, together with the acknowledgment of receipt for the notification. Category three data subjects will not be proactively informed, as ACER considers Article 20(1)(a) and (e) of the Regulation to be applicable in order to safeguard the investigation and ACER's regulatory tasks. Later, ACER provided a merged privacy statement covering both CMT and NP category two data subjects.

Information on category one data subjects will be kept for 10 years after they no longer are users of the NP and/or CMT. Information on category two and three data subjects will be kept for 10 years following closure of the case in CMT[4] and 10 years after the notification received in NP.

Personal data will only be accessible to the relevant persons working with the NP and CMT in ACER and the NRAs. They may be disclosed externally to the European Securities and Markets Agency (ESMA), national competition authorities, the European Commission and other competent authorities, as well as to judicial authorities. ACER has also entered into a

[3]Some MPs can be exempted from the prohibition of insider trading when they trade in wholesale energy products to cover immediate physical losses resulting from unplanned outages (Article 3(4)b) of REMIT) or can exceptionally delay the disclosure of an inside information (Article 4(2) of REMIT). In both cases, the REMIT regulation imposes to the MPs concerned to report/provide information and justification to ACER and the relevant NRA.

[4] Cases are closed when the competent national authority adopts a final decision.

memorandum of understanding with the Federal Energy Regulatory Commission (FERC) in the USA concerning the possible exchange of information. The privacy statements also mention possible disclosures to OLAF, the European Ombudsman, the Court of Justice, IAS and the EDPS. Transfers to recipients that do not have access to CMT or NP will be carried out by secured post.

Personal data may also be made available on an exceptional basis to external contractors which are considered as processors for ACER. These contractors are responsible for the development and maintenance, hosting services and to manage the Central Service Desk of the Agency for both CMT and NP. The contractors that host and support the operation of the systems have access to physical infrastructure, databases and storage media and the contractors that develop the systems may need to access the data to resolve the specific software related issues. The contractors are not allowed to access any data (including personal data), except once duly authorised by the Agency to do so. This authorisation may occur, for the contractors that host and support the operation of the systems, in case of problems with the systems or databases that will require the extraction of portions of the data to solve the issues. For the contractors that develop the systems, authorisation may occur in case of problems with the systems or databases that will require changes in the software to solve the issues.

While REMIT and the prohibitions of insider trading and market manipulation are already in force (and ACER has already received occasional reports/notifications), ACER has confirmed that the CMT is not in operation yet. ACER believes that the start of the trade and fundamental data collection on the 7th of October 2015 and of the monitoring of European energy markets will lead to significant change in the processing of personal data concerning REMIT, especially in quantitative terms. In this respect, ACER expects that the occasional suspicious reports/notifications received will increase notably.

3. Legal Analysis

3.1. Prior checking and Lawfulness of the processing

Article 27 of the Regulation contains the criteria for prior checking by the EDPS. Article 27(2)(a) lists processing involving certain categories of data, including "suspected offences, offences, criminal convictions" as subject to prior checking.

The NP and CMT are meant to process information on suspected breaches of REMIT, which are subject to either administrative or criminal penalties. This information falls under "suspected offences" in Article 27(2)(a). Both the NP where it is used to report suspected breaches[5] and CMT are therefore subject to prior checking.

However, the notification of exceptions and delays under Article 3(4) point b) and Article 4(2) of REMIT does not fall under Article 27 of the Regulation, as none of the criteria in that Article apply to these notifications.[6]

In order for the processing of personal data to be lawful, it has to be based on (at least) one of the grounds in Article 5 of the Regulation.

Article 5 (a) of the Regulation provides that personal data may be processed if the "processing is necessary for performance of a task carried out in the public interest on the

[5] Including reporting of delays/exemptions where ACER believes that delay/exemption is not justified and thus a suspected breach.

[6] Even though this part of the notification is not subject to prior checking, it has of course still to comply with the general rules on lawfulness, data subject rights, security etc.

basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof (...)". REMIT attributes certain tasks to ACER, which are implemented using the NP and CMT. The processing can thus be based on Article 5(a).

The notification also refers to Article 5(b), legal obligation, as a ground for lawfulness of the processing. The EDPS would like to point out that Article 5(b) only applies when the controller is under a legal obligation, which also specifies how the processing of personal data should be undertaken. This does not appear to be the case here.[7]

3.2. Processing of special categories of data

According to Article 10(5) of the Regulation, personal data relating to offences, criminal convictions or security measures may only be processed if authorised by the Treaties or other legal instruments.

Article 7(1) of the REMIT Regulation provides that ACER shall monitor trading activity in wholesale energy products to detect and prevent trading based on inside information and market manipulation. It shall collect the data for assessing and monitoring wholesale energy markets. Article 16 of the REMIT Regulation obliges NRAs to inform ACER when they have reasonable grounds to suspect that acts in breach of REMIT are or have been carried out. This provides an authorisation for ACER to receive this data and information. ACER will use this information in its monitoring and coordination roles and has confirmed that it does not carry out investigations on its own.

3.3. Data Quality

According to Article 4(1)(c) of the Regulation, personal data must be adequate, relevant and non-excessive in relation to the purposes for which collected and/or further processed.

The data categories processed in the NP and CMT appear to be adequate, relevant and non-excessive for the purposes pursued. ACER should take every reasonable step to ensure that personal data which are inaccurate or incomplete are erased or rectified.

3.4. Conservation of data

Article 4(1)(e) of the Regulation establishes that personal data must not be kept longer than is necessary for the performance of the task for which they were collected or further processed.

ACER has established a conservation period of ten years, starting from the closure of the case in CMT/notification using NP (data subject categories two and three) or from the moment a NP or a CMT user no longer uses the system (for category one data subjects). The reason given for data subject categories two and three is the possible need for follow-up.

However, not all cases will result in follow-up, for example those in which there were in the end no reasons to believe that a breach has occurred. For this reason, a blanket period of ten years appears excessive. Instead, **ACER should establish differentiated conservation periods depending on the outcome of the case**: cases which e.g. result in a review from a

[7] An example for processing whose lawfulness is based on Article 5(b) would be the annual publication of the declarations of interest of the members of ACER's Administrative Board (see Article 12(7) of Regulation 713/2009).

competent national authority are more likely to require follow-up on ACER's part than cases which do not result in such review.[8] .

3.5. Transfer of data

Transfers of personal data are subject to specific rules in Articles 7 to 9 of the Regulation. Article 7 applies for transfers of personal data within or between Community institutions or bodies; Article 8 to transfers to recipients, other than Community institutions and bodies, which are subject to (national legislation implementing) Directive 95/46/EC; Article 9 applies to other recipients, such as those in third countries or to national authorities in the Member States that do not fall under the legislation implementing Directive 95/46/EC.

3.5.1. Transfers under Article 7

Data from the NP and CMT will be transferred to a number of other Union institutions and agencies. According to Article 7, such transfers have to be necessary for the legitimate performance of tasks covered by the competence of the recipient; the recipient shall only use the data for the purposes for which they were transmitted.

Article 16(3)(b) of REMIT obliges ACER to transfer information (which may include personal data) to ESMA when it has reasonable grounds to believe that acts which constitute market abuse within the meaning of Directive 2003/6/EC and which affect financial instruments subject to Article 9 of that Directive are being or have been carried out. Such transfers can therefore be justified for the tasks carried out by ESMA in accordance with its mandate.

ACER also mentions transfers to the European Commission, referencing Article 16(3)(d) of REMIT. This Article obliges NRAs to inform their National Competition Authority (NCA), ACER and the Commission about suspected breaches of competition law. It does however not explicitly create a reporting channel from ACER to the Commission. According to the information provided by ACER, it might notify itself the relevant competent authority or the Commission if they become aware of a potential competition breach and the concerned NRA fails to do so, on the basis of the general cooperation obligation provided for in Article 1(3) of REMIT[9]

Transfers as explained above appear to be necessary for the recipient to carry out the tasks for which they are competent respectively.

3.5.2. Transfers under Article 8

ACER states that data from the NP and CMT may be transferred to a number of national authorities in the Member States.

ACER will primarily exchange data with the NRAs, since ACER monitors the market and NRAs investigate/enforce the REMIT Regulation. The fact that ACER, pursuant to Article

[8] See EDPS case 2014-0871, 2011-1127.

[9] "The Agency, national regulatory authorities, ESMA, competent financial authorities of the Member States, and where appropriate, national competition authorities shall cooperate to ensure that a coordinated approach is taken to the enforcement of the relevant rules where actions relate to one or more financial instrument to which Article 9 of Directive 2003/6/EC applies and also to one or more wholesale energy products to which Articles 3, 4 and 5 of this Regulation apply.".

16(4) of REMIT, can request information from NRAs or ask them to start an investigation de facto implies exchange of information/data.

REMIT obliges NRAs to transfer relevant information (which may include personal data) to different authorities in the Member States; depending on the case and suspected breach at hand, these may be competent financial authorities (Article 16(3) (a) and (b) REMIT), national competition authorities (Article 16(3)(d) REMIT) and other authorities or competent judicial authorities also entrusted with investigatory and enforcement powers (Article 13(1) REMIT).

For transfers to such authorities, ACER appears to be covered under Article 8(a) of the Regulation: the data appear to be necessary for the performance of a task carried out in the public interest or subject to the exercise of official authority of the recipient. It should be noted that Article 8 starts from the presumption that such transfers would be carried out upon request of the recipient. In the case at hand, however, the transfers will be carried out ex officio by ACER, which therefore is responsible for ensuring that these transfers will only happen to authorised recipients.

3.5.3. Transfers under Article 9

ACER has entered into a memorandum of understanding with the FERC, a US regulatory body. Additionally, ACER states that it may transfer personal data to judiciary and other investigatory authorities in the Member States.

Article 19 of REMIT empowers ACER to enter into administrative arrangements with third countries.

Transfers of personal data to recipients in third countries are subject to specific rules under Article 9 of the Regulation. Where there is no adequate level of protection ensured in the receiving country, transfer might still be possible under the derogations in Article 9(6).[10]

There is no relevant adequacy decision for the USA, and ACER neither appears to have carried out its own assessment of the adequacy of the safeguards provided, nor has it requested an authorisation under Article 9(7). This leaves the derogations in Article 9(6) of the Regulation as the only possible legal bases.

The only derogation that appears to possibly be relevant for CMT is Article 9(6)(d), which establishes a derogation according to which transfers may be allowed if the "transfer is necessary or legally required on important public interest grounds".

It has to be noted that the important public interest and legal requirement mentioned refer to those of the *sender*.[11] However, this is possible only on an exceptional basis. In other words, repeated, structural or massive data transfers cannot be justified under derogations.[12]

From the MoU between ACER and FERC, it is not clear whether such transfers will remain exceptional and could thus be covered under the derogation of Article 9(6)(d), or if they will be numerous enough to be considered repeated, massive or structural and would therefore require a different legal basis. Only if transfers remain exceptional the MoU can be sufficient.

[10] For a full explanation of the different possibilities for transferring personal data to third countries, see the EDPS position paper on the transfer of personal data to third countries, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf

[11] See p. 16 of the EDPS position paper cited above.

[12] See p. 15 of the EDPS position paper cited above.

For this reason, ACER shall report to the EDPS on the transfers carried out under Article 9(6) three, six and twelve months after the start of CMT.

If the transfers (whether to FERC or to any other third-country recipient) become repeated, massive or structural, ACER should suspend them until appropriate safeguards under Article 9 are implemented or an authorisation is granted.

The list of possible recipients mentioned by ACER also includes judicial authorities and investigatory bodies in the Member States. Not all of these are necessarily subject to national legislation implementing Directive 95/46/EC.[13] However, given that all Member States have implemented Council of Europe Convention 108, and have often extended the scope of their legislation implementing Directive 95/46/EC beyond the scope of the Directive, it could be considered that an "adequate" (or even "equivalent") level of protection exists in the areas of the former second and third pillar of EU law at national level. Therefore, transfers can take place under Article 9 as long as they respect the criteria of Article 8 of the Regulation.

Ratification of Council of Europe Convention 108 provides for a presumption of adequacy, which has to be verified in practice with the MS concerned. This will involve checking the concrete measures required of the recipient. For instance, are the police subject to specific data protection obligations, in line with Convention No. 108? Do they have a sufficient level of awareness about their data protection obligations? Are enforcement mechanisms applied when there is a breach? This analysis has to be documented by the controller.

Independently of the above, the EDPS notes that documenting transfers under Article 9 in an internal register is a good practice and encourages ACER to keep such a register, independently of the reporting requested in this Opinion (not only limited to CMT, but for all Article 9 transfers that may occur).

3.6. Right of access and rectification

According to Article 13 of the Regulation, data subjects have the right to access their own personal data and to have it rectified where incomplete or inaccurate. Restrictions may apply in line with Article 20.

ACER states that it will provide access and rectify where necessary; however, it notes that restrictions in line with Article 20 will be imposed for category three data subjects.

The EDPS would like to point out that such restrictions should only be imposed on a case-by-case basis and not as a general policy. The **justification for each restriction to the right of access should be documented internally.**

The justification should provide concrete reasons, linked to the specific case, as to why the application of a restriction is necessary. General considerations, such as simply quoting (parts of) Article 20 of the Regulation, are not enough.

It may also be necessary to have two parts to the justification. The reason is that under Article 20(3) of the Regulation, the data subject has to be informed of the principal reasons for the restriction. This should go beyond merely citing the relevant provisions of Article 20(1), but need not contain the full justification.

[13] See the EDPS position paper cited above, p. 22-23: being a pre-Lisbon first pillar instrument, the scope of the Directive excludes matters of criminal law.

The full reasoning should be documented internally at the time of applying the restriction, for example in a note to the file. This documentation should show why the restriction constitutes a necessary measure to safeguard the interests to be protected under Article 20(1) points (a) and/or (e) of the Regulation. Restrictions should be limited in time and should be reviewed (e.g. after a certain period of time, or when a file has reached a new stage).

Except for the point mentioned above, ACER appears to have put in place sufficient measures to grant the data subject the right of access and rectification.

3.7. Information to the data subject

In situations where data are collected from the data subject, they have to be informed in line with Article 11 of the Regulation; where data are not collected from the data subject, but from a different source, data subjects have to be informed in line with Article 12.

Category 1 and 2 data subjects are in the former situation, while category 3 data subjects are in the latter.

Concerning all privacy statements, the EDPS would like to mention the exception in Article 2(g) of the Regulation, establishing that authorities which may receive data in the framework of a particular inquiry are not to be considered recipients. The EDPS interprets this exception as applying to the information requirements under Articles 11 and 12.[14] In practice, this means that it is not necessary to mention the European Court of Auditors, the European Ombudsman, the EDPS, the Court of Justice of the European Union (General Court, Court of Justice and Civil Service Tribunal) and OLAF as entities that may receive personal data from CMT and NP.

Category one data subjects are only informed upon activation of their account. Article 11 implies that the information shall be provided at the latest when collecting the data. In the case at hand, this would mean already when collecting information for the user account request, not only when activating it. **Category one data subjects should already be informed when requesting the accounts.**

Similarly, category two data subjects only receive the data protection notice as part of the acknowledgment of receipt of their notification, i.e. after collection of their personal data. This information should be provided earlier, so that data subjects know how their data will be processed when submitting their report. **ACER should provide a link to the data protection notice in the notification form, or otherwise make sure that the information is provided in due time.**

Concerning ACERs proposal to merge the privacy statements for category two data subjects, there is no obligation to have separate ones. ACER is free to choose either way provided that the information required is included.[15]

Category three data subjects, falling under Article 12, should in principle be provided with the privacy statement at the time of the recording of their data. That being said, Article 12(2) contains some limitations to the scope of information obligations and there may be cases in which Article 20 may be used to restrict the right of information.

According to Article 12(2) controllers do not have to provide information under Article 12 where providing "such information proves impossible or would involve a disproportionate

[14] But not to the rules on transfers in Articles 7 to 9.
[15] Reducing the number of different privacy statements may be more efficient for ACER.

effort".[16] This exception aims at cases in which the personal data of the data subject do not allow contacting him/her, e.g. because no address or other means of contact are known. In such situations, the controller is usually not obliged to conduct further research to reach the data subject. Depending on the amount of information provided by the informant, this may apply to some categories of other data subjects mentioned in the notification submitted. It cannot, however, be assumed to be the case as a rule.

Where this exemption does not apply, such information may be delayed under Article 12 until the time of the first disclosure to a third party, where envisaged. As the CMT is meant to provide a coordination channel between ACER and NRAs, such disclosure is envisaged as part of the procedure. The obligation to inform thus applies at the latest in the moment of onward transfer to an NRA or other recipient (e.g. ESMA), unless ACER can apply a restriction under Article 20 of the Regulation.

Article 20(1) of the Regulation might justify restricting its application where necessary for safeguarding the "prevention, investigation, detection and prosecution of criminal offences" (point (a)).[17] This exception might be used where the alleged breaches have the status of criminal offences and informing the data subject at this stage would prejudice the investigation. The EDPS has interpreted the term "offences" in a wide manner to also include information related to disciplinary matters.[18]

Under Article 20(3), the principal reasons for these restrictions have to be communicated to the data subject. Article 20(5) allows deferring this information if providing it would deprive the restriction of its effect. However, any use of these exceptions must only occur on a case-by-case basis; blanket restrictions are not possible. The use of restrictions has to be justified and documented.

To summarise, there may be cases in which *some* data subjects other than informants may either fall under the limitations of the scope of the right to information under Article 12(2), or might be in situations where ACER would be entitled to restrict this right under Article 20. However, this cannot be assumed at a general level that *all* category three data subjects will fall into one of these cases. **ACER's approach of not informing data subjects other than informants as a matter of policy thus does not appear to be compliant with Articles 12 and 20**.[19] It should also be noted that being informed about the processing is a necessary precondition for exercising their other data subject rights. While there may very well be cases in which restrictions may be justified, this cannot be assumed to be the case on a policy level.

As it is likely that premature provision of this information could prejudice the investigation carried out by the NRA (or other recipient), ACER may -on a case-by-case basis- use the

[16] Article 12 also excludes •"recording or disclosure [which] is expressly laid down by Community law". This exception applies to cases in which there is a clear obligation in Community (now Union) law to record or disclose information not collected from the data subject. The fact that ACER is authorised by Union law to receive and forward information on suspected breaches of REMIT does not suffice to trigger this exemption, as it is only the possibility that is provided, and not the recording or disclosure of data relating to specific populations of data subjects.

[17] Point (e) is ancillary to this.

[18] By analogy to Article 13(1)(d) of Directive 95/46/EC, which includes "breaches of ethics for regulated profession".

[19] See also, by analogy, Article 29 Working Party Opinion 1/2006 concerning whistleblowing, page 13: "In particular, the reported employee must be informed about: [1] the entity responsible for the whistle blowing scheme, [2] the facts he is accused of, [3] the departments or services which might receive the report within his own company or in other entities or companies of the group of which the company is part, and [4] how to exercise his rights of access and rectification".

restrictions in Article 20. When these no longer apply, the data subject will have to be informed. When this will be the case depends on the state of the investigation carried out by the recipient. This recipient is the best-placed party to assess when this is the case.

As a pragmatic solution, the EDPS recommends **instructing recipients to include a link to ACER's relevant privacy statement when informing data subjects about their own processing,** thus ensuring that data subjects other than informants are appropriately informed about ACER's processing operations.[20]

3.8. Security measures and use of contractors

[…]

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the recommendations made in this Opinion are fully taken into account. To summarise, ACER should:

- establish differentiated conservation periods depending on the outcome of the case, with shorter periods for cases which do not result in a referral for follow-up;
- report to the EDPS on the transfers carried out under Article 9(6) three, six and twelve months after the start of CMT;
- if transfers to third country authorities become repeated, massive or structural, suspend them until appropriate safeguards under Article 9 are implemented or an authorisation is granted;
- justify each restriction to the right of access and document this justification internally;
- inform category one data subjects about the processing already when they request an account;
- provide a link to the data protection notice in the notification form for category two data subjects, or otherwise make sure that the information is provided in due time;
- instruct recipients to include a link to ACER's relevant privacy statement when informing data subjects about their own processing.

Done at Brussels, 02 October 2015

(signed)

Wojciech RAFAŁ WIEWIÓROWSKI

[20] The alternative would be to request recipients to inform ACER when they no longer see the need for a restriction, so that ACER could then proceed to inform data subjects on its own. This would create additional administrative burden compared to the suggested solution.