[doc. web n. 1628774]

Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator
Decision dated 27 November 2008, as published in Italy's Official Journal no. 300 of 24 December 2008 and amended by a Decision of the Italian DPA dated 25 June 2009 as published in Italy's Official Journal of 30 June 2009.

The Italian data protection authority

Having convened today, in the presence of Prof. Francesco Pizzetti, President, Mr. Giuseppe Chiaravalloti, Vice-President, Mr. Mauro Paissan and Mr. Giuseppe Fortunato, Members, and Mr. Giovanni Buttarelli, Secretary General;

Having regard to the Data Protection Code (decree no. 196 dated 30 June 2003), in particular section 31 et seq. and section 154(1)c. and h. thereof, as well as to the technical specifications on minimum security measures contained in Annex B to the said Code;

Having regard to official records concerning the protection of data processed with the help of IT systems and security of the data and systems in question;

Noting that it is necessary to undertake a specific action addressing the entities that are in charge of activities falling typically within the scope of those performed by the so-called "system administrators" as well as the entities discharging similar tasks in connection with processing systems and databases, in order to also highlight their importance vis-à-vis the processing of personal data and raise the awareness of both data controllers and the public at large as for the sensitiveness of the said tasks in the "Information Society" by having also regard to the attending risks;

Whereas it is necessary to facilitate, where appropriate, knowledge of the existence of professionals in charge of the above functions and/or similar functions as related to certain processing steps within bodies and organisations;

Considering that it is necessary to foster the adoption of specific precautions in discharging the tasks committed to system administrators along with technical and organisational measures and arrangements that should be aimed at facilitating compliance with the supervisory obligations vested in data controllers (due diligence);

Observing that the discharge of the duties committed to a system administrator, also where formally appointed as either a data processor or person in charge of the processing, entails, as a rule, the actual capability to access, whether intentionally or inadvertently, IT resources and personal data that a system administrator would not be entitled to access on account of the relevant authorisation profile;

Noting that it is necessary to bring the above risk to the attention of the public at large as well as of legal persons, public administrative bodies and any other bodies (hereinafter referred to as "data controllers" under section 4(1)f. of the DP Code) that rely on processing systems used by several persons in charge for different application and/or system-related functions to handle databases and/or IT networks;

Noting that data controllers are required under section 31 of the DP Code to take "suitable, preventative" security measures in connection with the processing operations they perform, whereby failure to take any such measures and/or to take suitable measures may result into their being liable under civil and/or criminal law (see sections 15 and 169 of the DP Code);

Observing that considerable importance should be attached to determining who qualifies for discharging the tasks of a system administrator, whereby this is actually one of the key decisions that – along with those related to technologies – enhance the overall security of the processing operations in question and should be accordingly taken care of by avoiding ill-advised appointments;

Whereas the data controller, if deciding to avail himself of the option to appoint one or more data processors, is required to only appoint entities that "can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters." (see section 29(2) of the DP Code);

Considering that the controllers of data processing operations performed in the public and/or private sectors for management and accounting purposes, which entail lesser risks to data subjects and were accordingly

the subject of recent simplification measures (see section 29 of decree no. 112 dated 25 June 2008 as converted, with amendments, into Act no. 133 dated 6 August 2008; see also section 34 of the DP Code and the Italian DPA's decision dated 27 November 2008), should fall outside the scope of application of this decision;

Having regard to the considerations submitted by the Secretary General on behalf of the Office as per Article 15 of the Regulations no. 1/2000;

Acting on the report submitted by Prof. Francesco Pizzetti;

WHEREAS

1. Preliminary Remarks

In the IT sector, a "system administrator" is usually a professional in charge of managing and servicing a processing system and/or components thereof. For the purposes of this decision, the scope of the above definition will be enlarged to include other professionals that can be equated in terms of data protection risks – such as database administrators, network and security equipment administrators, and the administrators of complex software systems.

System administrators defined as above are usually not in charge of operations that require them to understand the relevant application domain – i.e., data meaning, representational format, functional semantics; however, it is often the case that they are de facto "in charge" for specific processing steps that may entail considerable data protection criticalities.

Technical activities such as data backup/recovery, management of network flows, handling of storage media and/or hardware maintenance entail, in many cases, the capability to impact on information; such capability should be equated, for all intents and purposes, to the processing of personal data – even if the administrator does not access "plaintext" information.

The importance, peculiarities and criticalities attached to the functions of system administrators have also been taken into account by Parliament, which has considered the discharge of certain technical functions – albeit termed differently – as an aggravating circumstance applying to the commission of certain offences. Reference can be made, in particular, to the misuse of one's tasks as system operator that is mentioned in the Criminal Code regarding the offence of unauthorised access to an IT system and/or electronic networks (Section 615-ter) and computer fraud (Section 640-ter) as well as in connection with the offences consisting in damaging information, data and software on electronic networks (Sections 635-bis and 635-ter) and damaging IT systems and electronic networks (Sections 635-quater and 635-quinquies), which were recently amended.

The data protection legislation prior to enactment of the 2003 consolidated Code defined system administrators as the entities "in charge for supervising over the resources of the operating system of a computer and/or database and for enabling such resources to be used" (see section 1(1)c. of Presidential decree no. 318/1999).

Conversely, there is no definition of system administrator in the DP Code in force. Nevertheless, the functions typically committed to system administrators are mentioned in Annex B to the DP Code, whereby data controllers are required to ensure safekeeping of the confidential components of authentication credentials. A large chunk of the tasks set out in the said Annex fall typically within the scope of system administrators' functions – from the creation of backup copies (data backup and recovery operations) to safekeeping of credentials, to management of authentication and authorisation systems.

Overall, the aforementioned provisions highlight the peculiar powers vested in system administrators and the trust-based relationship underlying their activities – a situation that is similar, albeit in a totally different context, to certain safekeeping activities and other functions that may only be discharged by persons meeting specific technical and organisational requirements as also related to their conduct, professional skills and/or ethical standards; to date, such requirements are not taken into account in connection with one of the most difficult tasks in the "Information Society".

In the course of the inspections carried out by the Italian DPA over the past few years, it could be appreciated that most companies and major public and private organisations attach considerable importance to system administrators (as well as to network and database administrators) – even apart from legal requirements; the functions applying to such administrators are set out in security plans and/or security policies and, in some cases, the administrators in question are appointed as data processors.

Conversely, it could be found that in other cases – not only concerning small-sized businesses – there was no sufficient awareness of the criticalities applying to the discharge of the tasks in question; this resulted

worryingly into underestimating the risks arising out of the unsupervised activities of administrators, who are supposed to also monitor and control the appropriate use of IT systems.

Accordingly, the Italian DPA is issuing this decision to call upon all the controllers of processing operations that are performed, in whole or in part, with the help of electronic tools to take due account of the need for considering the risks and criticalities related to committing the tasks of system administrators.

Additionally, the Italian DPA considers that it is necessary to specify hereby an initial set of organisational measures that should make it easier for public and private bodies and organisations to become aware of the existence of certain technical functions, of the responsibilities vested in such functions and, in some cases, of the identity of the individuals working as system administrators in connection with the various services and databases at issue.

2. Regulatory Framework
This decision relies, in particular, on Section 154(1)h. of the DP Code, whereby one of the tasks entrusted to the Italian DPA consists in raising "public awareness of the legislation applying to personal data processing and the relevant purposes as well as of the data security measures."

Under Section 154(1)c., the Italian DPA is additionally empowered to lay down such measures and arrangements, whether general or specific, as data controllers are required to implement.

3. Calling upon Data Controller's Attention Vis-à-Vis the Tasks Committed to System Administrators
Under Section 154(1)h. above, the Italian DPA calls upon all data controllers falling within the scope of application of the DP Code, where they process personal data with the help of electronic tools, to take account of the peculiar criticalities related to the functions discharged by system administrators and draws their attention hereby to the need for taking suitable precautions in order to prevent and detect unauthorised accesses to the personal data in question – in particular where such accesses take place by misusing the powers committed to system administrators. Additionally, the Italian DPA highlights the need for taking special care in committing technical functions that correspond and/or are similar to those discharged by system administrators, where such functions are carried out in a context that allows personal data to be accessed, whether inadvertently or not, via the available technical facilities. In doing so, account should be taken of the advisability of committing the functions in question as well as of the specific mechanisms applying to discharge of the said functions along with the technical, professional and behavioural qualifications of the given candidate. The assessment in question should be performed by also considering the liability that may arise under Criminal and Civil Law (see sections 15 and 169 of the DP Code) if the appointment is performed inappropriately and/or unwarily.

4. Measures and Arrangements Imposed on the Controllers of Processing Operations Performed with the Help of Electronic Tools
The measures and arrangements to be implemented under section 154(1)c. of the DP Code by all the controllers of processing operations concerning personal data that are carried out with the help of electronic tools are specified hereinafter. The requirements in question do not apply to processing operations performed in the private and/or public sector for management and accounting purposes, as such operations were the subject of recent simplification measures on account of the lesser risks for data subjects (see Act no. 133/2008; section 34 of the DP Code; and the DPA's decision dated 6 November 2008).

The arrangements and measures below are without prejudice to additional specific precautions that may be required by sector-related legislation in respect of certain processing operations and/or may be provided for subsequently by the Italian DPA in pursuance of section 17 of the DP Code.

4.1. Assessing Personal Qualifications
Prior to proceeding with the appointment of an individual as system administrator, it is necessary to assess the candidate's experience, skills and reliability; the candidate will have to provide suitable assurances that he/she will comply in full with the data protection legislation in force as also related to security issues.

The data controller and data processor must abide by assessment standards that are equivalent to those applying to the appointment of data processors under section 29 of the DP Code, regardless of whether the functions of system administrator (or similar functions) are only committed in connection with the appointment as person in charge of the processing pursuant to section 30 of the DP Code.

4.2. Individual Appointment
The appointment as system administrator must be performed on an individual basis; it is necessary to detail the scope of the activities the given administrator is allowed to carry out based on the relevant authorisation profile.

4.3. List of System Administrators
Information required to identify the natural persons working as system administrators including a list of the functions committed to them must be reported in an internal document that should be updated regularly and made available for inspection by the Italian DPA.

If the activities performed by system administrators concern, also indirectly, services or systems that process and/or allow processing personal information on employees, private and public employers acting as data controllers are required to disclose and/or allow disclosure of the identity of system administrators within the respective organisations – depending on the features of the given company or service – by having regard to the various IT services such administrators are in charge of.

To that end, they may rely on the information notice they are to provide to their employees - i.e. the data subjects - under section 13 of the DP Code; alternatively, they may avail themselves of the technical specifications that are to be adopted pursuant to the DPA's decision no. 13 dated 1 March 2007 (as published in Italy's Official Journal no. 58 dated 10 March 2007) or else make use of internal communication tools such as the corporate intranet, circular letters and/or bulletins. This is without prejudice to any items of legislation that rule out the disclosure and/or communications mentioned above and provide for different rules in respect of a specific sector.

If system administration services are outsourced, the data controller, or else the data processor, is directly responsible for keeping the information required to identify the natural persons appointed as system administrators.

4.4. Regular Checks
Data controllers or else data processors must check system administrators' activities at least annually to verify that they are compliant with the organisational, technical and security measures provided for in the legislation in force applying to the processing of personal data.

4.5. Access Logging
Systems must be in place to log accesses (computer authentication) to processing systems and electronic databases as performed by system administrators. In terms of their completeness, non-modifiability and amenability to integrity controls, the access logs must be such as to allow achieving the purposes of the checking activity for which they are intended.

The access logs must include timestamps and event descriptions; they must be retained for a suitable period which shall not be shorter than six months.

5. Timeframe for Implementing Measures and Arrangements
Regarding the controllers of processing operations that have already started and/or are to start within thirty days as from the date of publication of this decision in the Official Journal, the measures and arrangements referred to in paragraph 4 will have to be implemented as quickly as possible and anyhow by no later than one-hundred and twenty days as from the aforementioned date.

Regarding any other processing operation that starts after thirty days from the aforesaid date of publication in the Official Journal, the measures and arrangements in question will have to be implemented prior to start of the data processing operations.

NOW, THEREFORE, BASED ON THE ABOVE PREMISES THE ITALIAN DATA PROTECTION AUTHORITY

1. Under Section 154(1)h. of the DP Code, calls upon all the controllers of processing operations concerning personal data that fall within the scope of application of the DP Code and are carried out with the help of electronic tools, to take account of the peculiar criticalities related to the functions discharged by system administrators. The Italian DPA draws their attention hereby to the need for taking special care in committing technical functions that correspond and/or are similar to those discharged by system administrators, database administrators and/or network administrators where such functions are carried out in a context that allows personal data to be accessed, whether inadvertently or not, via the available technical facilities. In doing so, account should be taken of the advisability of committing the functions in question as well as of the specific mechanisms applying to discharge of the said functions along with the technical, professional and behavioural qualifications of the given candidate;

2. Under Section 154(1)c. of the DP Code, orders that the following measures and arrangements be implemented by all the controllers of processing operations concerning personal data that fall within the scope of application of the Code and are carried out with the help of electronic tools, as also related to processing operations in the judicial and police sectors (see Sections 46 and 53 of the DP Code). The

requirements in question do not apply to processing operations performed in the private and/or public sector for management and accounting purposes, as such operations were the subject of recent simplification measures on account of the lesser risks for data subjects (see Act no. 133/2008; section 34 of the DP Code; and the DPA's decision dated 6 November 2008):

a. Assessing Personal Qualifications
Prior to proceeding with the appointment of an individual as system administrator, it is necessary to assess the candidate's experience, skills and reliability; the candidate will have to provide suitable assurances that he/she will comply in full with the data protection legislation in force as also related to security issues.

The data controller and data processor must abide by assessment standards that are equivalent to those applying to the appointment of data processors under section 29 of the DP Code, regardless of whether the functions of system administrator (or similar functions) are only committed in connection with the appointment as person in charge of the processing pursuant to section 30 of the DP Code.

b. Individual Appointment
The appointment as system administrator must be performed on an individual basis; it is necessary to detail the scope of the activities the given administrator is allowed to carry out based on the relevant authorisation profile.

c. List of System Administrators
Information required to identify the natural persons working as system administrators including a list of the functions committed to them must be reported in an internal document that should be updated regularly and made available for inspection by the Italian DPA.

If the activities performed by system administrators concern, also indirectly, services or systems that process and/or allow processing personal information on employees, private and public employers acting as data controllers are required to disclose and/or allow disclosure of the identity of system administrators within the respective organisations – depending on the features of the given company or service – by having regard to the various IT services such administrators are in charge of.

To that end, they may rely on the information notice they are to provide to their employees - i.e. the data subjects - under section 13 of the DP Code; alternatively, they may avail themselves of the technical specifications that are to be adopted pursuant to the DPA's decision no. 13 dated 1 March 2007 (as published in Italy's Official Journal no. 58 dated 10 March 2007), make use of internal communication tools such as the corporate intranet, circular letters and/or bulletins, or else implement standardised procedures at the employee's request. This is without prejudice to any items of legislation that rule out the disclosure and/or communications mentioned above and provide for different rules in respect of a specific sector.

d. Outsourced Services
If system administration services are outsourced, the data controller or else the external data processor are directly responsible for keeping the information required to identify the natural persons appointed as system administrators.

e. Regular Checks
Data controllers or else data processors must check system administrators' activities at least annually to verify that they are compliant with the organisational, technical and security measures provided for in the legislation in force applying to the processing of personal data.

f. Access Logging
Systems must be in place to log accesses (computer authentication) to processing systems and electronic databases as performed by system administrators. In terms of their completeness, non-modifiability and amenability to integrity controls, the access logs must be such as to allow achieving the purposes of the checking activity for which they are intended. The access logs must include timestamps and event descriptions; they must be retained for a suitable period which shall not be shorter than six months.

3. Orders that the measures and arrangements referred to in paragraph 2 hereof be implemented – as regards processing operations that have already started and/or are to start within thirty days as from the date of publication of this decision in the Official Journal – as quickly as possible and anyhow by no later than one-hundred and twenty days as from the aforementioned date; as for any other processing operation that starts after thirty days from the aforesaid date of publication in the Official Journal, the measures and arrangements in question will have to be implemented prior to start of the data processing operations;

3-bis. Orders that the task of implementing the measures set forth in point 2, letters d. and e. be conferred on the data processor, if any, within the framework of the appointment of the latter by the data controller as per section 29 of the DP Code, or else via appropriate contractual clauses;

4. Orders that a copy of this decision be sent to the Ministry of Justice – Ufficio pubblicazione leggi e decreti in order for it to be published in the Official Journal of the Italian Republic.

Done in Rome, this twenty-seventh day of the month of November 2008.

THE PRESIDENT
Pizzetti

THE RAPPORTEUR
Pizzetti

THE SECRETARY GENERAL
Buttarelli