## Annex 5: Standard Contractual Clause

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:

Address:

Tel.: Fax: Email:

Other information needed to identify the organization:

---

(the data exporter)

And

Name of the data importing organization: Shindig, Inc.

Address: 433 Broadway - Suite 505, New York, NY 10013 USA

Tel.: Fax: Not Applicable Email:
Other information needed to identify the organization: a _____ corporation

---

(the data importer)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1*

*Definitions*

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(b) '*the data exporter'* means the controller who transfers the personal data;

*(c)* *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

*(d)* *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

*(f)* *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*

*Obligations of the data exporter*

**The data exporter agrees and warrants:**

**(a)** **that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;**

**(b)** **that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;**

**(c)** **that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;**

**(d)** **that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;**

**(e)** **that it will ensure compliance with the security measures;**

**(f)** **that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;**

**(g)** **to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;**

**(h)** **to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;**

**(i)** **that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and**

**(j)** **that it will ensure compliance with Clause 4(a) to (i).**

*Clause 5*

*Obligations of the data importer*[2]

**The data importer agrees and warrants:**

[2] **Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions,**

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

*Clause 6*

***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7*

***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*

***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established,
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

---

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

| |
|---|
| Signature: |
| (Stamp of Organization) |

**On behalf of the data importer:**

Name (written out in full):

Position: Chief Financial Officer

Address: 433 Broadway - Suite 505, New York, NY 10013 USA

Other information

| |
|---|
| Signature: |
| (Stamp of Organization) |

necessary in order for the contract to be binding (if any):

# Appendix 1

**to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):
Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses (SCC) as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased SCC Services on the basis of one or more Order Form(s).

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):
Shindig, Inc. ("SHINDIG") is a provider of virtual meeting room services which processes personal data upon the instruction of the data exporter according to the Service Agreement. Personal data may be collected according to the Services Agreement to support the SHINDIG service, and the processing activity may involve collection, storage, duplication, electronic viewing, deletion and destruction of personal data. SHINDIG is located in the United States of America, and all data exported will be exported to SHINDIG in the United States of America. The data controller grants its consent to the export of data to the data importer in the United States of America.

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data of data subjects which may include:

- employees of the data exporter and its affiliates,
- including partners and contractors and,
- exporter's meeting participants.

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

**Provisioning Data**: The following provisioning data is collected to establish services for Shindig video users. This information is stored and associated with an individual's profile.

- Contact Name
- Email Address
- Phone Number
- Geographic Location

- Dialing Address

**Meeting Metadata:** The following information is collected only if a person uses the portal to schedule a meeting and invite other participants.

- Meeting Title
- Meeting participant names
- Call log details
    - Display name of participants
    - Inbound URIs and/or IP addresses of participants
    - Call duration

**Conference Media:** The following media may be processed during any videoconferencing session:

- Audio streams
- Video streams
- Content sharing
- Online presence

**Meeting Chat Messages:** The following information may be collected if a person uses the chat tool to relay instant messages to others or groups attending the meeting.

- Participant Name
- Chat Message
- Timestamp of Message
- Files transferred (when applicable)

**Reporting Data:** The following information is stored in a database to facilitate generating a report for the purpose of support and audit, and to provide utilization metrics in regards to the Shindig service.

- Meeting Title
- Meeting Participant Names
- Call Log Details
    - Display Name of Participants
    - Inbound URIs and/or IP Addresses of Participants
    - Call Duration

**Recording When Applicable:** The following information is only applicable if a user records a video meeting; this must be initiated by the users, and at the time of recording initiation, all participants in the meeting are notified that the session is being recorded.

- Name
- Email Address
- Call Log Details (Display name, URI, duration, stream title, stream viewer IP, IP address);
- Virtual Meeting Room Dialing Information
- Virtual Meeting Room Pin Code (if applicable)
- Customer meta data (Meeting title, meeting participant names, index tag)
- Audio Media
- Video Media
- Content Sharing Media

**Support Data:** The following data could be associated with incident management (ticketing), if a user opens a ticket with the support desk and requests help to redress a conference issue.

- Contact Name
- Email Address
- Phone Number
- Geographic location
- Call/Meeting Data
- Device logs
    - Call log details if applicable for troubleshooting, which usually includes H323 and SIP call negotiation and maintenance events from the local and remote terminals.
    - Device specific details such as applications, operating system, hardware components, performance metrics, and firmware, application names for applications that are able to be shared from the end users device, global contact/address lists associated to the device.

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Shindig service, specifically as a meeting title or within a chat message, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is, for the sake of clarity, Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):
Personal data may be collected according to the Services Agreement to support the Shindig service, and the processing activity may involve collection, storage, duplication, electronic viewing, deletion and destruction of personal data.

DATA EXPORTER

Name: ...
Authorized Signature ...

DATA EXPORTER

Name: ...

Authorized Signature ...

DATA IMPORTER

Name: ...

Authorized Signature ...

# Appendix 2

**to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

Data importer maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data input into the virtual meeting room services. These security measures are cemented in an Information Security Management System (ISMS) for the purpose of protecting Personal Data and information, primarily with a view to meeting pre-defined requirements of applicable data protection and privacy law across Controller markets. These requirements have largely been derived from legislation across Controller markets mandating fundamental security measures for the protection of Personal Data and are intended to provide a harmonized and single standard.

These requirements are applied for the protection of Personal Data on behalf of the Controller.

**Security Officer**

1. A person responsible for the overall compliance with these minimum-security requirements shall be designated as the Security Officer. This person shall be suitably trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.
2. The contact details of the Security Officer shall be promptly provided to the

Controller. **Security Plan and Document**

3. The measures adopted to comply with these minimum-security requirements shall be the subject of a security plan and set out in a security document, which shall be kept up to date, and revised whenever relevant changes are made to the Information System or to how it is organized. The security document shall record significant changes to the security measures or the processing activities.
4. The security plan shall address: Security measures relating to the modification and maintenance of the system used to Process Personal Data, including development and maintenance of applications, appropriate vendor support and an inventory of hardware and soft Physical security, including security of the buildings or premises where data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls.
5. Data security mechanisms for securing the integrity and confidentiality of the data, classification of the data.
6. Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system, mechanisms for keeping account of attempts to break system security or gain unauthorized access.
7. The security plan shall include:
    a. a Disaster Recovery Plan which shall set out: measures to minimize interruptions to the normal functioning of the system; limit the extent of any damage and disasters; enable a smooth transition of Personal Data from one computer system to another; if necessary, provide for alternative means of operating a computer system; educate, exercise and familiarize personnel with emergency

procedures; provide for fast and smooth system recovery, and minimize the economic effects of any disaster event.

b. a Contingency Plan which must address the following possible dangers to the system and appropriate criteria to determine when the Plan should be triggered: the critical functions and systems, the strategy for protecting the system and priorities in the event the Plan is activated; an inventory of relevant staff members to be called upon during an emergency, as well as telephone numbers of other relevant parties; a set of procedures for calculating the damage incurred; realistic time management plans to enable the recovery of the system; clearly allocated staff duties; possible use of alarms and special devices (e.g., air filters, noise filters); in the event of a fire, special equipment should be available (e.g., fire extinguisher, water pumps, etc.); devices or methods for determining temperature, humidity and other environmental factors (e.g., air conditioning, thermometers, etc.); special security software to detect breaches of security; special generators for dealing with power cuts; retention of copies of software or materials in other protected buildings to avoid inadvertent loss.

8. The security document shall be available to staff who have access to Personal Data and the Information Systems, and must cover the following aspects as a minimum:

    a. The scope, with a detailed specification of protected resources;

    b. The measures, standards, procedures, code of conduct rules and norms to guarantee security, including for the control, inspection and supervision of the Information Systems;

    c. The functions and obligations of staff;

    d. The structure of files containing Personal Data and a description of the Information Systems on which they are Processed;

    e. The purposes for which the Information Systems may be used;

    f. The procedures for reporting, managing and responding to incidents;

    g. The procedures for making back-up copies and recovering data including the person who undertook the process, the data restored and, as appropriate, which data had to be input manually in the recovery process.

9. The security document and any related records and documentation shall be retained for a minimum period of 5 years from the end of the Processing.

**Functions and Obligations of Staff**

10. Only those employees who have demonstrated honesty, integrity and discretion should be Authorised Users or have access to premises where Information Systems or media containing Personal Data are located. Staff should be bound by a duty of confidentiality in respect of any access to Personal Data.

11. The necessary measures shall be adopted to train and make staff familiar with these minimum-security requirements, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Personal Data and the consequences of any breach of these requirements.

12. The functions and obligations of staff having access to Personal Data and the Information Systems shall be clearly defined and documented.

13. Authorised Users shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during Processing sessions.

14. Physical access to areas where any Personal Data are stored shall be restricted to Authorised Users.

15. The disciplinary measures for a breach of the security plan shall be clearly defined and documented and communicated to staff.

**Authorisation**

16. Only those employees who have a legitimate operational need to access the Information Systems or carry out any Processing of Personal Data shall be authorised to do so ("Authorised Users").
17. An authorisation system shall be used where different authorisation profiles are used for different purposes.

**Identification**

18. Every Authorised User must be issued with a personal and unique identification code for that purpose ("User ID").
19. A User ID may not be assigned to another person, even at a subsequent time.
20. An up-to-date record shall be kept of Authorised Users, and the authorised access available to each, and identification and authentication procedures shall be established for all access to Information Systems or for carrying out any Processing of Personal Data.

**Authentication**

21. Authorised Users shall be allowed to Process Personal Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.
22. Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorised User; alternatively, authentication shall consist in an authentication device that shall be used and held exclusively by the person in charge of the Processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the Processing and may be associated with either an ID code or a password.
23. One or more authentication credentials shall be assigned to, or associated with, an Authorised User.
24. There must be a procedure that guarantees password confidentiality and integrity. Passwords must be stored in a way that makes them unintelligible while they remain valid. There must be a procedure for assigning, distributing and storing passwords.
25. Passwords shall consist of at least eight characters, or, if this is not technically permitted by the relevant Information Systems, a password shall consist of the maximum permitted number of characters. Passwords shall not contain any item that can be easily related to the Authorised User in charge of the Processing and must be changed at regular intervals, which intervals must be set out in the security document. Passwords shall be modified by the Authorised User to a secret value known only to the Authorised User when it is first used as well as at least every six months thereafter.
26. The instructions provided to Authorised Users shall lay down the obligation, as a condition of accessing the Information Systems, to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by Authorised Users are kept with due care.
27. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management and support purposes.
28. Authentication credentials shall be also de-activated if the Authorised User is disqualified or de-authorised from accessing the Information Systems or Processing Personal Data.
29. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the controller can ensure that data or electronic equipment are available in case the person in charge of the Processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their

confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Such entities shall have to inform the person in charge of the Processing, without delay, as to the activities carried out.

**Access Controls**

30. Only Authorised Users shall have access to Personal Data, including when stored on any electronic or portable media or when transmitted. Authorised Users shall have authorised access only to those data and resources necessary for them to perform their duties.
31. A system for granting Authorised Users access to designated data and resources shall be used.
32. Authorisation profiles for each individual Authorised User or for homogeneous sets of Authorised Users shall be established and configured prior to the start of any Processing in such a way as to only enable access to data and resources that are necessary for Authorised Users to perform their duties.
33. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply. This may also include the list of Authorised Persons drawn up by homogeneous categories of task and corresponding authorisation profile.
34. Measures shall be put in place to prevent a user gaining unauthorised access to, or use of, the Information Systems. In particular, firewalls and/or intrusion detection systems reflecting the state of the art and industry best practice should be installed to protect the Information Systems from unauthorized access. Measures shall be put in place to identify when the Information Systems have been accessed or Personal Data has been Processed without authorization, or where there have been unsuccessful attempts at the same.
35. Operating system or database access controls must be correctly configured to ensure authorised access.
36. Only those staff authorised in the security document shall be authorised to grant, alter or cancel authorised access by users to the Information Systems.

**Management of Media**

37. Information Systems and physical media storing Personal Data must be housed in a secure physical environment. Measures must be taken to prevent unauthorized physical access to premises housing Information Systems.
38. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and Processing.
39. Media containing Personal Data must permit the kind of information they contain to be identified, Inventoried (including the time of data entry; the Authorised User who entered the data and the person from whom the data was received; and the Personal Data entered) and stored at a physical location with physical access restricted to staff that are authorised in the security document to have such access.
40. When media are to be disposed of or reused, the necessary measures shall be taken to prevent any subsequent retrieval of the Personal Data and other information stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means, before they are withdrawn from the inventory. All reusable media used for the storage of Personal Data must be overwritten three times with randomised data prior to disposal or re-use.
41. The removal of media containing Personal Data from the designated premises must be specifically authorised by the controller.
42. Media containing Personal Data must be erased or rendered unreadable if it is no longer used or prior to disposal.

**Distribution of Media and Transmission**

43. Media containing Personal Data must only be available to Authorised Users.

44. Printing/copying Processes must be physically controlled by Authorised Users, to ensure that no prints or copies containing Personal Data remain left in the printers or copying machines.

45. Media containing Personal Data or printed copies of Personal Data must contain the classification mark "Confidential".

46. Encryption (128-bit or stronger) or another equivalent form of protection must be used to protect Personal Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Personal Data in a physically insecure environment.

47. Paper documents containing Personal Data must be transferred in a sealed container / envelope that indicates clearly that the document must be delivered by hand to an Authorised User.

48. When media containing Personal Data are to leave the designated premises as a result of maintenance operations, the necessary measures shall be taken to prevent any unauthorised retrieval of the Personal Data and other information stored on them.

49. A system for recording incoming and outgoing media must be set up which permits direct or indirect identification of the kind of media, the date and time, the sender/recipient, the number of media, the kind of information contained, how they are sent and the person responsible for receiving /sending them, who must be duly authorised.

50. Where Personal Data is transmitted or transferred over an electronic communications network, measures shall be put in place to control the flow of data and record the timing of the transmission or transfer, the Personal Data transmitted or transferred, the destination of any Personal Data transmitted or transferred , and details of the Authorised User conducting the transmission or transfer.

**Preservation, Back-up copies and Recovery**

51. Tools must be in place to prevent the unintended deterioration or destruction of Personal Data.

52. Procedures must be defined and laid down for making back-up copies and for recovering data. These procedures must guarantee that Personal Data files can be reconstructed in the state they were in at the time they were lost or destroyed.

53. Back-up copies must be made at least once a week, unless no data have been updated during that period. **Anti-Virus / Intrusion Detection**

54. Anti-virus software or intrusion detection systems should be installed on the Information Systems to protect against attacks or other unauthorised acts in respect of Information Systems. Antivirus software and intrusion detection systems should be updated regularly in accordance with the state of the art and industry best practice for the Information Systems concerned (and at least every six months).

**Software Updates**

55. The software, firmware and hardware used in the Information Systems shall be reviewed regularly in order to detect vulnerabilities and flaws in the Information Systems and resolve such vulnerabilities and flaws. This review shall be carried out at least annually.

**Access Record**

56. A history of Authorised Users' access to or disclosure of Personal Data shall be recorded on a secure audit trail.

**Physical Access Record**

57. Only those staff duly authorised in the security document may have physical access to the premises where Information Systems and media storing Personal Data are stored. A record of staff who access such premises shall be maintained, including name, date and time of access.

**Record of Incidents**

58. There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches or attempts at unauthorised access. This shall include as a minimum:

    a. A procedure for reporting such incidents/ breaches to appropriate management within the processor;

    b. A clearly designated team for managing and co-ordinating the response to an incident led by the Security Officer;

    c. A documented and tested process for managing the response to an incident including the requirement to keep appropriate issues and action logs to include the time at which the incident occurred, the person reporting the incident, to whom it was reported and the effects thereof;

    d. The requirement on the processor to notify the controller immediately if it appears that Personal Data was involved in the incident or breach or may be impacted or affected in some way; and

    e. The processor security/ incident management team should where appropriate work together with the controller's security representatives until the incident or breach has been satisfactorily

resolved.