DPA eDisplay srl

2021

Summary

MASTER DATA PROCESSING AGREEMENT (MDPA)
(from EU Regulation 2016/679)

This Data Processing Agreement (the "Agreement") is entered into between Edisplay Srl, referred to as the "Supplier" or "Data Processor" or "eDisplay," and the Client, as identified below, in accordance with the provisions of Article 28 of EU Regulation 2016/679, hereinafter also referred to as the "GDPR." The terms set forth herein constitute an appendix and supplement to the provisions of the contract(s) executed between the parties for the supply of one or more products and/or services by Edisplay. The parties are identified as follows:

- "Supplier" (also referred to as the "Supplier," the "Data Processor," or "eDisplay"): Edisplay Srl, with registered office in Fonni (NU) at Viale del Lavoro No. 53, VAT and Tax Code 01172340919, represented by its pro tempore legal representative, Raffaele Serusi;
- "Customer" (also referred to as the "Customer" or the "Owner"): The individual specified in the contract(s) through which the Customer has acquired one or more products and/or services from the Supplier, governing the terms and conditions thereof.

The terms "Supplier" and "Customer" collectively shall be referred to as the "Parties," and each individually as a "Party."

WHEREAS,

a. The Customer has entered into one or more contracts (hereinafter the "Contract") with the Supplier, focused on the purchase of one or more products and/or services offered by the Supplier, the details of which are fully referenced for any unspecified aspects in this Agreement;

b. The Parties intend to outline in this "Master Data Processing Agreement" (hereinafter referred to as the "MDPA" or "Agreement") the terms and conditions governing the processing of personal data conducted by the Provider within the framework of the Contract and the provision of the Services, as well as the responsibilities related to such data processing, including the commitments undertaken by the Provider as the Data Processor, in accordance with Article 28 of the GDPR. The provisions of this MDPA are complemented, as necessary, by a specific Data Processing Agreement (DPA) corresponding to each product/service. If prepared, the DPA is provided to the Customer concurrently with this Agreement;

c. The Customer has determined that the Supplier possesses the requisite reliability, capability, and experience to ensure compliance with the prevailing provisions on the processing of personal data.

By entering into the relevant contract for the provision of one or more services offered by the Supplier, the Customer declares full acceptance of the following conditions.

1. DEFINITIONS AND INTERPRETATION

The preamble is an integral part of this Agreement. In this Agreement, the following terms and expressions shall have the meanings associated with them below:

- **"Agreement Effective Date"** means the date on which the Customer enters into or accepts this Agreement.
- **"Personal Data"** has the meaning set out in the Personal Data Protection Legislation and includes all data processed by the Provider as a result of the Contract. This encompasses all data provided, stored, sent, received, or otherwise processed or created by the Customer, as well as by the End User in connection with the use of the Services.
- **"Adequacy Decision"** means a decision of the European Commission on the basis of Article 45(3) of the GDPR, determining whether the laws of a certain country ensure an adequate level of protection as required by the Personal Data Protection Legislation.
- **"Notification Address"** means the email address(es) and/or certified email address(es) provided by the Client at the time of subscribing to the Service or provided through another official channel to the Supplier and used for receiving notifications from the Supplier.
- **"Instructions"** means the written instructions given by the Owner in this Agreement and, where applicable, in the Agreement.
- **"Legislation on the Protection of Personal Data"** means the GDPR and any additional rules, implementing regulations issued pursuant to the GDPR, or in force in Italy regarding the protection of Personal Data. This includes any binding provision issued by the competent supervisory authorities on the protection of Personal Data (e.g., the Guarantor for the protection of personal data), including the requirements of the General Authorisations for the processing of sensitive and judicial data, if applicable and maintaining their binding effect after May 25, 2018.
- **"Supplier Personnel"** means the Supplier's officers, employees, consultants, and other authorized personnel, excluding the personnel of Additional Data Processors.
- **"Request"** means any request by a data subject falling within those provided for in the Legislation on the Protection of Personal Data (e.g., exercise of rights, complaints).
- **"Additional Data Processor"** means any third party processing personal data on behalf of the Data Processor, whether the Customer is the Data Controller with respect to the same data or the Customer is the Data Processor and the Supplier has the status of an additional Data Processor with respect to the latter.
- **"Service(s)"** means the service(s) and any products covered by the Contract(s) entered into between the Customer and the Supplier from time to time.
- **"End User"** means the end user, if any, of the Service, who is the Data Controller.
- **"Personal Data Security Breach"** means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data occurring on systems operated by the Provider or over which the Provider has control.
- **"Terms and Conditions"** means a commercial agreement referenced in this "Agreement."

2. ROLE OF THE PARTIES

2.1. The Parties acknowledge and agree that, for the purposes set out in the Contract, the Supplier acts as a Data Processor ("Processor") pursuant to Art. 28 of the GDPR, and the Client acts as the Data Controller of the Personal Data ("Controller").

2.2. If the Client carries out processing operations on behalf of another Data Controller, the Client may act as a Data Processor. In such a case, the Customer warrants that the instructions given and the activities undertaken in relation to the processing of Personal Data, including the appointment by the Customer of the Supplier as an additional Data Processor resulting from the conclusion of this Agreement, have been authorized by the relevant data controller and undertakes to exhibit, upon the Supplier's written request, the documentation certifying the above.

2.3. Each Party undertakes to comply, in the processing of Personal Data, with their respective obligations deriving from the applicable Personal Data Protection Legislation.

2.4. The Supplier is expressly authorized to make use, where necessary, of Additional Data Processors. The Provider warrants, in such a case, that the same data protection obligations imposed on it under this MDPA will be imposed on such processors.

2.5. The Data Controller is required to ensure that the processing of Personal Data referred to in the Contract is carried out in accordance with the Legislation on the Protection of Personal Data.

3. PROCESSING OF PERSONAL DATA

3.1. By entering into this Agreement, the Client entrusts the Supplier with the task of processing Personal Data for the sole purpose of providing the Services as further detailed in the Agreement and in this Agreement.

3.2. Access to Personal Data is aimed at pursuing an exclusive interest of the Data Controller, and Personal Data will not be used in any way for the pursuit of the Controller's own purposes. For each processing carried out, the Data Processor undertakes to implement the security measures provided for by the Legislation on the Protection of Personal Data and not to act for illegal purposes.

3.3. The Supplier undertakes to comply with the Instructions and to comply with all the obligations provided for by the Personal Data Protection Legislation for the Supplier, understanding that if the Client requests variations from the initial Instructions, the Supplier will evaluate the feasibility aspects and agree with the Client on the aforementioned variations and the related costs.

3.4. In cases referred to in Art. 3.3 and in the event of requests by the Customer involving the processing of Personal Data that are, in the opinion of the Supplier, in violation of the Legislation on the Protection of Personal Data, the Supplier is entitled to refrain from carrying out such Instructions and will promptly inform the Customer. In such cases, the Client may evaluate any changes to the Instructions given or contact the Supervisory Authority to verify the lawfulness of the requests made.

.

4. LIMITATIONS ON THE USE OF PERSONAL DATA

4.1. When processing Personal Data for the purpose of providing the Services, the Provider undertakes to process Personal Data:

- a. only to the extent and in the manner necessary to provide the Services or to properly fulfill its obligations, provided for by the Contract and this Agreement or imposed by the Legislation on the Protection of Personal Data. In the latter circumstance, the Supplier will inform the Customer (unless prohibited by law for reasons of public interest) by means of a notice sent to the Notification Address;
- b. in accordance with the Customer's Instructions.

4.2. The Supplier's Personnel who access or otherwise process Personal Data are responsible for processing such data on the basis of appropriate authorizations and have also received the necessary training regarding the processing of Personal Data. Such personnel are also bound by confidentiality obligations and the Company's Code of Ethics and must comply with the confidentiality and personal data protection policies adopted by the Supplier ("Authorized Parties").

5. PROVISIONS ON THE SECURITY OF THE PROVIDER AND RIGHTS OF THE DATA SUBJECTS

5.1. When processing Personal Data for the purpose of providing the Services, the Provider shall take appropriate technical and organizational measures to minimize the risks of unlawful or unauthorized processing, accidental or unlawful destruction, damage, accidental loss, alteration, or unauthorized disclosure of, or access to, Personal Data, as described in Annex 1 to this Agreement ("TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES" or "Annex 1").

5.2. Annex 1 to the Agreement contains data storage protection measures commensurate with the level of risks present with respect to Personal Data to enable the confidentiality, integrity, availability, and resilience of the Provider's systems and Services, as well as measures to enable the timely restoration of access to Personal Data in the event of a Personal Data Security Breach, and measures to test the long-term effectiveness of those measures. The Client acknowledges and accepts that, taking into account the state of the art, the costs of implementation, as well as the nature, scope, context, and purposes of processing of the Personal Data, the security procedures and criteria implemented by the Provider ensure a level of protection appropriate to the risk with regard to its Personal Data.

5.3. The Supplier may update and modify the Security Measures indicated above over time, it being understood that such updates and modifications may not result in a reduction in the overall level of security of the Services.

5.4. If the Client requests additional security measures, the Supplier reserves the right to assess feasibility and, prior to possible implementation, will agree in good faith with the Data Controller any additional costs.

5.5. The Supplier, considering the nature of the processing and the information at its disposal, assists the Client in ensuring compliance with the security obligations referred to in Art. 32-36 of the GDPR as defined in this agreement.

5.6. The Supplier guarantees that all the necessary technical and organizational measures will be put in place to ensure an adequate level of security commensurate with the degree of risk.

5.7. If the product/service covered by the Contract allows operation with third-party applications (e.g., Google Sheets, eCommerce products) that the Client can freely choose to use, the responsibility for this choice remains with the Client, and the Supplier cannot be held responsible for the application of suitable Security Measures in the components of third parties or for the methods of operation of the same and compliance, in general, with the GDPR by the third party.

5.8. The Data Controller, taking into account the nature of the processing, shall assist the Data Controller with appropriate technical and organizational measures, to the extent possible, to meet the latter's obligation to follow up on requests for the exercise of the data subject's rights referred to in Chapter III GDPR. The Data Controller acknowledges and accepts that the management of relations with data subjects remains its responsibility, and it is therefore the Data Controller itself who must respond to such requests or any complaints. If a data subject is contacted directly, the Data Processor collects the requests, recommending the data subject to contact the Customer directly, as the Data Controller. At the same time, the supplier communicates the request/complaint received to the Data Controller by email, accompanying it with any information that is not already available to the Data Controller and that is necessary for the processing of the request/complaint.

5.9. If the Client needs to receive information from the Data Processor (which is not already in its possession)

in order to demonstrate compliance with the obligations referred to in Art. 28 GDPR, as a result of a request received from the Supervisory Authority, the Supplier will make such information available within the deadline imposed by the Authority. It is understood that, in order for this deadline to be respected, the request must be promptly notified to the Data Protection Officer (who can be contacted at the email address indicated above) and to the Supplier itself.

6. CUSTOMER SECURITY MEASURES

6.1. Without prejudice to the obligations set out in paragraph 5 above for the Supplier, the Client acknowledges and accepts that, in using the Services, it remains solely responsible for adopting adequate security measures by its staff and those authorized to access said Services.

6.2. To this end, the Client undertakes to use the Services and related functionalities to ensure a level of protection appropriate to the actual risk.

6.3. The Client also undertakes to take all appropriate measures to protect the authentication credentials, systems, and devices used by the Client or by users at the End User's premises to access the Services. The Client further commits to saving and backing up Personal Data to ensure the restoration of Personal Data in compliance with the law.

6.4. Any obligation or responsibility on the part of the Supplier regarding the protection of Personal Data stored or transferred by the Customer or the End User, if applicable, outside the systems used by the Supplier and its Additional Data Processors (e.g., in paper archives, or in its own data centers, as in the case of Contracts concerning products installed at the Customer's premises or at the Customer's suppliers) is excluded.

7. SECURITY BREACHES

The Provider, if it becomes aware of a Personal Data Security Breach:

7.1. Informs the Client without undue delay and, in any case, no later than 24 hours after becoming aware of the violation by means of a communication sent to the Notification Address.

7.2. Takes reasonable measures to limit foreseeable harm to data subjects and the security of Personal Data.

7.3. Provides the Client with a description of the Personal Data Security Breach that has occurred and informs the Client:

- a. The nature of the breach (including, where possible, the categories and approximate number of data subjects and records of the data in question);
- b. The likely consequences of the personal data breach and the measures taken or proposed to be taken to remedy the breach, including to mitigate its possible adverse effects.

If, and to the extent that, it is not possible to provide all the information at the same time, the Data Processor shall communicate to the Data Controller the information available at that time, and the other information shall be provided subsequently, as soon as it is available, without undue delay.

7.4. Considers as confidential the information relating to any Security Breaches, the related documents, press releases, and notices and does not communicate data or information relating to them to third parties without the prior written consent of the Data Controller, except in cases strictly necessary for the fulfillment

of regulatory obligations (of any kind) on the Client or the Supplier itself, requests from the competent authorities, the fulfillment of contractual obligations, the mitigation of risks that may be borne by the data subjects, or activities instrumental to the aforementioned purposes.

7.5. The Client acknowledges and accepts that it is his/her sole responsibility to fulfill, as Data Controller, in the cases provided for by the Legislation on the Processing of Personal Data, any obligations to notify the Supervisory Authority and the data subjects of the Security Breach.

7.6. It is understood that the notification of a Security Breach or the taking of measures to deal with a Security Breach does not constitute an acknowledgment of default or liability on the part of the Supplier in relation to such Security Breach.

7.7. The Client, in the event of a Security Breach, shall promptly notify the Supplier of any misuse of accounts or authentication credentials, as well as any unauthorized use of the Services the Client uses and of which the Client has become aware.

8. APPOINTMENT OF ADDITIONAL MANAGERS

8.1. With this agreement, the Data Controller grants the Supplier general authorization to use additional data processors (Sub-Processors), in compliance with the provisions of Art. 28 (2) and (4) GDPR. This authorization does not extend to cases involving the transfer of data outside the European Union or to international organizations, a transfer that can only take place upon the fulfillment of the conditions referred to in paragraph 9 below. The Data Processor expressly undertakes to inform the Data Controller of any changes regarding the addition or replacement of any Sub-processors, giving him the opportunity to object to such changes. The Data Processor may not resort to the Sub-processors in relation to which the Data Controller has expressed its opposition.

8.2. In the event that the Processor uses a Sub-processor for specific activities, the same obligations referred to in this MDPA will be imposed on such Sub-processor through the stipulation of a contract or other legal act of equivalent value in Italian law, ensuring sufficient guarantees in the adoption of the necessary technical and organizational measures to ensure that the processing complies with the provisions of the GDPR.

8.3. The Additional Data Processors are kept by the Data Processor in a special register in digital format and can also be consulted remotely by the Data Controller upon request

9. RESTRICTIONS ON THE TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

9.1. The Supplier stores and processes Personal Data for which the Client is the Data Controller within the European Union and does not transfer Personal Data outside the EEA unless the conditions specified in Art. 9.2.

9.2. If the Supplier intends to transfer, even for storage purposes only, the personal data covered by this agreement outside the European Union or to International Organizations, it shall notify the Client at least 60 days in advance. If the Client does not consent to the transfer, the Client may withdraw from the contract within 15 days of such notice. If the Client does not exercise this right of withdrawal within the aforementioned term, the Data Processor may transfer the above data in compliance with the conditions set out in Art. 44 et seq. GDPR.

10. CHECKS AND CONTROLS

10.1. The Supplier shall periodically audit the security of the systems and environments for the processing of Personal Data used by the Supplier for the provision of the Services and the locations where such processing takes place. The Supplier shall have the right to appoint independent professionals selected by the Supplier to carry out audits according to international standards and/or best practices, the results of which will be reported in specific reports ("Reports"). Such Reports, constituting confidential information of the Supplier, may be made available to the Customer upon request to enable it to verify the Supplier's compliance with the security obligations set out in this Agreement.

10.2. The Client agrees that, in the cases referred to in clause 10.1, its right of verification will be exercised through the verification of the Reports made available by the Supplier.

10.3. The Supplier acknowledges the Client's right, in the manner and within the limits indicated below, to carry out independent audits periodically to assess the organizational, technical, and security measures adopted by the Data Processor as well as to verify the Supplier's compliance with the obligations set forth in this Agreement and with the regulations in force on the processing of personal data. The Client may use its own specialized personnel or external auditors for these activities, provided that these subjects are previously bound by appropriate confidentiality commitments. By this agreement, the Client guarantees that confidentiality is respected by the appointed auditors.

10.4. The Client shall first send a written request for verification (audit) to the Head of the Data Protection (DPO) of the Supplier through the address indicated in this agreement or, if applicable, subsequently replacing and at the same time as the Supplier itself (at the addresses indicated in the Contract or subsequently communicated in place of the same).

10.5. The Supplier may object in writing to the appointment by the Client of any external auditors whom it considers to be inadequately qualified or independent, who are competitors of the Supplier, or who are manifestly inadequate. The supplier must always be able to assist, also through its own qualified personnel or external auditors appointed by the same, in the conduct of audit activities.

10.6. It is understood that the audits referred to in this point may only be conducted in relation to the areas involved in the data processing processes for which the Client is the Data Controller.

10.7. The Client undertakes to indemnify the Supplier against any costs that may arise from the performance of the audit. Any such costs will have to be examined jointly by the parties when planning the audit. The costs of the verification activities commissioned by the Client to third parties remain the sole responsibility of the Client.

10.8. The Supplier has appointed a Data Protection Officer, who can be contacted at the email address: dpo@edisplay.it. The supplier will take care to inform the Customer of any change in the contact details indicated.

11. COMPLIANCE ASSISTANCE

11.1. The Supplier, taking into account the nature of the Personal Data processed, undertakes to assist the Client in ensuring compliance with the obligations referred to in Art. 32-36 GDPR. In particular, it will provide assistance to the Client and cooperate in the manner indicated below to allow the Client to comply with the obligations provided for by the Legislation on the Protection of Personal Data.

11.2. The Supplier shall promptly inform the Client, unless prohibited by law, by notifying the Notification Email of any inspections or requests for information submitted by supervisory authorities and police forces with respect to profiles concerning the processing of Personal Data.

11.3. If, for the purpose of processing the Requests referred to in the previous points, the Client needs to receive information from the Supplier regarding the processing of Personal Data, the Supplier will provide the necessary assistance by providing the information at its disposal.

11.4. The Supplier, taking into account the nature of the Personal Data and the information available to it, will provide assistance to the Client in making available useful information to enable the Client to carry out impact assessments on the protection of Personal Data in the cases provided for by law. In such a case, the Provider will make available all information necessary under the Service and clearly requested by the Customer, such as the information contained in the Agreement, this Agreement, and any additional DPAs. Any requests for personalized assistance may be subject to the payment of a fee by the Customer. It is understood that it is the sole responsibility and burden of the Customer, or of the End User if the Data Controller, to proceed with any necessary/appropriate Impact Assessments (DPIA) relating to the processing of Personal Data carried out by the same in the context of the Services.

12. CUSTOMER'S OBLIGATIONS AND LIMITATIONS

12.1. The Client undertakes to give Instructions in accordance with the regulations and to use the Services in accordance with the Personal Data Protection Legislation and only to process Personal Data that has been collected in accordance with the Personal Data Protection Legislation.

12.2. The Client undertakes to fulfill all the obligations imposed on the Data Controller.

12.3. It is the Client's responsibility to keep the account linked to the Notification Email active and up to date.

13. DURATION, RETURN DELETION OF PERSONAL DATA

13.1. This Agreement is valid from the date of signing of the Contract to which it refers and until such time as all Personal Data is deleted by the Data Processor, based on the provisions set out in paragraph 13.2 below.

13.2. At the end of the expiry of the Contract and/or in the event of its termination, the Personal Data owned by the Data Controller held by the Data Processor and any copies of the Data themselves, including those provided by the Data Controller through direct entry into the Supplier's online platform, will be kept for a period of 6 months, so as to still be available if the same Service is reactivated in the period following the expiry and to guarantee the exercise of the right to portability, unless there is an obligation under national and/or European law or regulation that provides for the storage of such Data. In any case, the Data Controller may request early cancellation at the end or termination of the contract, as well as personally proceed with the cancellation if the service provides for the possibility (e.g.: Emailchef).

13.3. Retention for 6 months following the conclusion of the relationship is not guaranteed and is not the subject of any claim by the Data Controller, once the right of portability has been exercised. After this period, the data will be deleted and no copy will be kept, unless storage is necessary on the basis of a regulatory obligation. In this case, the data will be stored for the period prescribed by the individual provision. In addition, any data necessary for the establishment, exercise, or defense of a right in court will be stored until the expiry of the relevant limitation period

14. RESPONSIBILITIES

14.1. Each Party is responsible for the fulfilment of its obligations under this Agreement

15. CATEGORIES OF DATA CONCERNED

15.1. Personal data that the Client has provided to the Controller may be processed, including by archiving directly on the Supplier's portal for the purpose of using the chosen services.

15.2. Typically, common personal data are processed, such as: personal data, contact data, or data indicating the work activity carried out, bank details.

15.3. The above data mainly refer to the following categories of data subjects: customers and potential customers, suppliers, employees, and collaborators.

15.4. Additional data and even special data (e.g., data relating to health) may be processed, also referring to other subjects identified by the Data Controller who has verified the existence of a suitable legal basis and other conditions necessary for the lawfulness of the processing and its compliance with the GDPR.

15.5. The Client undertakes not to communicate in any way to the Supplier personal data with respect to which it cannot guarantee that the processing is lawful and, in general, compliant with the GDPR in compliance with the principle of Accountability and the responsibilities that, based on this principle, are borne by the Data Controller.

16. EQUIVALENT

16.1. The consideration agreed in the Contract includes the services inherent in the position of Data Processor.

17. APPLICABLE LAW AND JURISDICTION

17.1. This Agreement is governed by Italian law.
17.2. Any dispute that may arise with reference to the execution, interpretation and/or application of this Agreement shall be subject to the exclusive jurisdiction of the Court of Nuoro.

18. VALIDITY OF THIS AGREEMENT AND AMENDMENTS

18.1. The provisions of this Agreement supersede and supersede any contractual or other matters that may be entered into between the parties on the same matter. If the Supplier decides to make one or more changes to this agreement, it will notify the Client in writing, also by electronic means (e-mail, PEC). In this case, if the Client does not agree to the changes made, the Client may withdraw from the Contract within 60 days of receipt of such notice. The withdrawal must be communicated in writing by registered mail with acknowledgment of receipt or by certified email. Failure to do so will be deemed accepted and binding for both parties.

19. COMMUNICATIONS & NOTIFICATIONS

19.1. Any communication between the parties concerning the Processing of Personal Data must be made to the addresses communicated at the time of the stipulation of the contract or possibly subsequently communicated in substitution.

Milano, 27.05.2021

THE DATA PROCESSOR
eDisplay srl

THE LEGAL REPRESENTATIVE
Raffaele Serusi

TECHNICAL AND ORGANISATIONAL MEASURES (Annex 1)

In addition to the security measures provided for in the Contract and in the MDPA, the Data Processor applies the following organizational security measures depending on the type of Service with which the product is provided or licensed:
A – Cloud SaaS

Measurements of safety Organizational	**User Policies and Regulations** – The Supplier applies detailed policies and regulations, to which all users with access to information systems have the obligation to comply and which are aimed at ensuring to ensure compliance with the principles of confidentiality, availability and data integrity in the use of computing resources. **Logical Access Authorization –** the Supplier defines the access profiles in the compliance with the least privilege necessary for the execution of the assigned tasks. Authorization profiles are discovered and configured prior to the start of the processing, so as to limit access only to the data necessary for the carry out the processing operations. These profiles are subject to periodic checks aimed at verifying the the conditions for the preservation of the assigned profiles are met. **Service Incident Management** – Service incidents are regulated in order to ensure that only the activities envisaged are carried out contractually and prevent the overprocessing of personal data whose ownership is the responsibility of the Customer or End User. **Data Protection Impact Assessment (DPIA)** – In accordance with art. 35 and 36 of the GDPR and based on WP248 – Guidelines on Data Protection Impact Assessment adopted by the Working Group pursuant to Article 29, the Supplier has prepared its own methodology for the analysis and the evaluation of the processing that, considering the nature, the object, the context and the purposes of the processing, present a high risk to the rights and freedoms of natural persons for the purpose of proceeding with the assessment

	the impact on the protection of personal data before commencing the processing. **Incident Management** – The Supplier has implemented a specific incident management procedure Incident Management to ensure the restoration of normal service operations in the shortest possible time, ensuring the maintaining the best levels of service. **Data Breach** – The Supplier has implemented a specific procedure aimed at the management of events and incidents with a potential impact on data roles and responsibilities, the survey process (presumed or established), the enforcement, response and containment of the incident/violation as well as the modalities through the such as to communicate personal data breaches to the Client. **Training**: The Supplier periodically provides its employees involved with in the processing activities, training courses on the correct management of data Personal
Measurements of Technical safety Measurements of Technical safety	**Firewall, IDPS** - Personal data is protected against the risk of intrusion by pursuant to art. 615-quinquies of the Criminal Code by means of Intrusion systems Detection & Prevention, kept up-to-date in relation to the best available technologies. **Security Lines of Communication**- To the extent of their competence, they are adopted by the Supplier secure communication protocols in line with the provisions of the Technology makes it available. **Protection from malware** – Systems are protected against the risk of intrusion and the action of programmes through the activation of appropriate instruments updated on a regular basis. Antivirus tools are in use and are constantly updated. **Authentication credentials** – Systems are configured in a suitable way to allow access only to persons with authentication that allow them to be uniquely identified. These include, code associated with a keyword, reserved and known only to the same; authentication device in the exclusive possession and use of the user, possibly associated with an identification code or a keyword. **Keyword** – With regard to the basic characteristics, i.e. the obligation to Modification at first access, minimum length, absence of elements easily traceable to the subject, rules of complexity, deadline, history, contextual assessment of robustness, visualization and Storage, the keyword is managed in accordance with best practices. To Subjects to whom the credentials are attributed are provided with precise instructions in relation to the arrangements to be adopted to ensure its secrecy. **Logging –** Systems are configurable in ways that allow the tracking of access and, where appropriate, of the activities carried out by the different types of users (Administrator, Super User, etc.) protected by adequate security measures to ensure its integrity. **Backup & Restore** – Appropriate measures are taken to ensure recovery access to data in the event of damage to data or tools electronically, within certain timeframes compatible with the rights of the data subjects. Where contractual arrangements provide for this, a continuity plan shall be put in place integrated operations, where necessary, with the disaster recovery plan; they ensure availability and access to the systems even in the event of events significant negative effects that should persist over time. **Vulnerability Assessment & Penetration Test** – The Supplier carries out periodic vulnerability analysis activities aimed at detecting the state of exposure to known vulnerabilities, both in relation to scopes infrastructure and applications, considering the systems in operation or in operation development phase.

Measurements of Technical safety	Where deemed appropriate in relation to the potential risks identified, these audits are periodically integrated with specific Penetration techniques Testing, using intrusion simulations using different attack, with the aim of verifying the security level of applications/systems/networks through activities that aim to exploit the vulnerabilities detected to circumvent physical/logical security mechanisms, and have access to them. The results of the checks shall be examined in detail in order to identify and implement the necessary points of improvement to ensure the high level of security required. **System Administrators** – Relating to all users who work in as System Administrators, whose list is kept up to date and the whose functions are appropriately defined in specific acts of appointment, a log management system is managed in order to ensure that the tracking of the activities carried out and the storage of such data with unalterable modalities suitable for ex post monitoring. The work of System Administrators is subject to verification activities in order to check compliance with organisational, technical and security measures with respect to the processing of personal data provided for by current regulations. **Data Center** – Physical access to the Data Center is limited to individuals only Authorized. For details of the security measures adopted with reference to the data centers provided by the Additional Data Processors, as well as identified in the MDPA Special Conditions, reference is made to the security measures described by the same Additional Data Processors and made available in the related institutional websites at the following addresses (or those that will be subsequently made available by the Additional Managers): **For Data Center services provided by Amazon Web Services**: https://aws.amazon.com/it/compliance/data-center/controls/ For datacenter services provided by Microsoft: https://www.microsoft.com/en-us/trustcenter **Protection from malware VMs** – VMs are protected against the risk of intrusion and the action of programmes through the activation of appropriate instruments to be updated periodically. All VMs are managed through antivirus features (both at the hypervisor level and infrastructural). **Backup & Restore** – Appropriate measures are taken to ensure recovery access to data in the event of damage to data or tools electronically, within certain timeframes compatible with the rights of the data subjects.
	High reliability – the Supplier guarantees high reliability in the following terms: • The Server architecture is based on the use of the VMWare virtualization applied through physical duplication, and of individual systems, in order to ensure fault tolerance and the elimination of single points of failure. In particular, in the case of failure of a system, the virtual environment management software is able to redistribute ongoing activities to other systems (high availabilty and load balancing), minimising disruptions and ensuring the persistence of existing connections. • Each server is attested on a SAN via an iSCSI connection to High speed. • All components of the infrastructure are fully redundant to eliminate any single point of failure. • The network architecture is designed to protect frontend systems from the Internet

	and internal networks through the use of a DMZ protected by two distinct firewalling layers (defense-in-depth): a border firewall connected to the Internet and a second firewall, which it also integrates Intrusion Prevention and anti-malware features, owned by the organisation, is put in place to protect the DMZ and its backend systems. All alarms are remotely controlled by the security guard.