DATA PROTECTION POLICY

Lottomatica Group

LOTTOMATICA

CONTENTS

1. INTRODUCTION

In carrying out its activities, the Lottomatica Group (i.e. Lottomatica Group S.p.A. and/or one of the other companies of the Group controlled by it) collects personal data from its customers, employees, suppliers, users, job applicants, investors, partners and other third parties.

Each company in the Lottomatica Group conducts its personal data collection and processing activities in compliance with all applicable laws and in line with the highest standards of conduct. Data protection has always been at the heart of the Group's commitment to all stakeholders and is a core value that inspires the conduct of the Lottomatica Group, contributes to the success of its business, and consolidates customer and investor confidence in it.

The Lottomatica Group closely and constantly monitors regulatory developments in order to adapt its activities from time to time to the EU Regulation 679/2016 of April 27, 2016. In particular, over the years, specific interventions have been planned with regard to the implementation of technical and organizational measures aimed at protecting the personal data processed; updating the suppliers that carry out personal data processing activities on behalf of Group companies; and updating impact assessments for specific types of processing activities.

In order to further strengthen its social commitment and focus on the care and welfare of people and consumer protection, on May 13, 2022, the Board of Directors of Lottomatica Group S.p.A. formally approved the internal regulation on the "Processing of personal data and free circulation of data in accordance with European regulation 2016/679" and the procedure on "Data breach management & notification", both of which are addressed to personnel belonging to the entire Lottomatica Group, which together with the notices (the main ones of which are attached) and the operating procedures already in place at Group companies and referred to in the documents constitute the Data Protection Policy.

A further step in the path of continuous improvement and compliance with privacy regulations by the Lottomatica Group is the achievement, by the companies Gamenet S.p.A. and Gbo Italy S.p.A., of ISO/IEC 27701:2019 certification, which recognized compliance with the international standard of the information security and privacy management system in use at the companies.

2. OBJECTIVES

This Policy ("**Policy**"), in addressing all interested parties to the data processing put in place by the Lottomatica Group (i.e. Lottomatica Group S.p.A. and/or one of the other companies of the Group controlled by it) aims to describe the internal processes adopted by the Group in order to ensure that processing activities are carried out in compliance with the data protection standards outlined in EU Regulation 679/2016 (GDPR).

In order to achieve this objective, the Lottomatica Group makes this Policy available to all its data subjects and processors, within which the main regulations, disclosures, and privacy procedures in use within the Lottomatica Group are encapsulated, which all recipients undertake to comply with.

3. ADDRESSEES AND SCOPE OF APPLICATION

This Policy is addressed to and applies to the personal data of customers, employees, suppliers, users, job applicants, investors, partners and other third parties subject to processing by the Lottomatica Group (i.e. Lottomatica Group S.p.A. and/or one of the other Group companies controlled by it) as well as to personal data processed by suppliers and third parties contracted on behalf of the Lottomatica Group.

4. INTERESTED PARTIES

The categories of data subjects addressed by this Policy are:

- Suppliers and contractual third parties;
- Customers;
- Employees and collaborators;
- Applicants;
- Investors.

5. PROCESSING OF PERSONAL DATA AND FREE CIRCULATION OF DATA IN ACCORDANCE WITH EUROPEAN REGULATION 2016/679

5.1 PURPOSE

The Lottomatica Group issues the following procedure with regard to the processing of personal data and the free circulation thereof pursuant to European Regulation 2016/679 and its implementing rules ("GDPR"), in order to define the Group's roles, responsibilities and main operating procedures for protecting personal data and adequately managing the risks involved in data processing. In this respect, the Lottomatica Group guarantees that this procedure and the data processing governed by it is in compliance with the principles described in the following sub-section.

5.1.1 PRINCIPLES APPLICABLE TO THE PROCESSING OF PERSONAL DATA

The Lottomatica Group ensures that the processing of personal data is consistent with the principles set out in Article 5 of Regulation (EU) 2016/679.

Lawfulness, correctness, and transparency
The data subjects' personal data is processed in a lawful, correct manner and for purposes explicitly described by the Data Controller in the privacy policy.

Processing is legitimate if specific conditions are met, including:

- execution of a contract;
- the pursuit of a legal obligation and/or the legitimate interest of the Data Controller or a third party (provided, in the latter case, that the data subject's right to protection is not overridden);
- the data subject's expression of consent.

Data subjects (e.g. player customers and/or employees) are adequately informed of the existence and possibility of asserting their rights with regard to the use of their data, the identity of the data controller and the purposes for which the data is processed.

Purpose limitation
The Lottomatica Group ensures that personal data is processed only for determined, explicit and legitimate purposes, both in the collection and in the other activities of which the processing is part and, in particular, the registration, storage, editing, consultation, use and disclosure.

Data minimisation
The information collected (in terms of the amount of data collected, the extent of the processing and the period of accessibility and storage of the data) is limited to the extent necessary for the purposes for which it is processed.

Accuracy
The personal data processed are accurate and, if necessary, are updated; the Lottomatica Group takes all reasonable measures to promptly delete or rectify data that is inaccurate in relation to the purposes for which it is processed if requested by the data subject and if permitted by law.

Retention limitation
The data subjects' personal data is stored in a manner that allows it to be identified, for no longer than is necessary for the data controller to fulfil its purposes or to comply with legal obligations (e.g. gambling, tax, anti-money laundering regulations, etc.).

Accountability
The Group Companies, in their capacity as Data Controllers and/or Data Processors, implement appropriate and effective measures for the protection of data, taking into account the nature, scope, context and purposes of the processing.

Integrity and confidentiality
Personal data is adequately protected against unauthorised processing and accidental loss or modification. To maintain security and prevent processing in violation of the provisions of current legislation, Group companies, data controllers and processors assess the risks inherent to processing and implement appropriate measures to limit the risks.

5.1.2 SCOPE

The Regulation specifies rules relating to the protection of individuals with regard to the processing of personal data, as well as rules relating to the free circulation of such data, protecting the fundamental rights and freedoms of natural persons. The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing of personal data not by automated means contained in or intended to be contained in a filing system.

The GDPR is applied to the processing of personal data: (i) carried out as part of the activities of an establishment by a Data Controller or a Data Processor in the European Union, regardless of whether or not the processing is carried out in the European Union; (ii) of data subjects located in the European Union, carried out by a Data Controller or a Data Processor who is not established in the European Union, where the processing activities relate to the offering of goods or the provision of services to such data subjects in the European Union or to the monitoring of their conduct to the extent that this conduct takes place within the European Union. In this context, this procedure represents the corporate framework for the processing of personal data, with particular reference to the security measures to protect processing by automated and non-automated means. Furthermore, this procedure provides the operating instructions regarding the main personal data protection requirements, such as:

a) Acknowledgement of the data subjects' exercise of rights;
b) The keeping and updating of the register of processing operations;
c) The management of personal data breaches (so-called "data breach");
d) The data protection impact assessment.

This procedure is to be applicable to the Lottomatica Group (as defined below), without prejudice to the specific features of each Group company with reference to the nature of its corporate purpose and any specific regulations.

5.2 RECIPIENTS

This procedure is intended for personnel, system administrators, interns and collaborators with employment contracts, consultants from external companies or independent contractors, any recurring visitors and in general all those who process personal data belonging to and/or under the responsibility of Gamenet S.p.A. and the companies of the Lottomatica Group (to which Gamenet S.p.A. belongs), within the limits set out in section 2 above.

5.3 DEFINITIONS AND ASSOCIATED DOCUMENTS

The following terms and definitions have the meaning ascribed to each of them below, it being specified, however, that terms defined in the singular form shall also be understood as defined in the plural form and vice versa. It being understood that further terms, other than those defined herein, shall have the meaning attributed to them by the EU Regulation 2016/679 and its implementing rules. For the purposes of this procedure the following are defined:

- **System Administrators**, means the natural persons entrusted with the task of supervising the management of a Processing System (e.g. database administrators, network and security equipment administrators and administrators of complex software systems);
- **GDPR**, means EU Regulation 2016/679 of the European Parliament and Council of 27 April 2016, as amended and supplemented; **Privacy Code**, means Legislative Decree 196 of 30 June 2003, as last amended by Legislative Decree 101 of 10 August 2018, as amended and supplemented;
- **Disclosure**, means the disclosure of personal data to one or more persons other than the data subject, the controller's representative in the territory of the State, the controller and the persons authorised to process the data, in any form, including by making them available, consulting them or linking them;
- **Personal data** or **Data**, means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by reference in particular to an identifier such as a name, an identification number, location data, an online identifier or data referring to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.
- **Dissemination**, means giving knowledge of personal data to unspecified persons, in any form, including by making the data available or consulting it;
- **Supervisory Authority** or **Guarantor**, is the Italian Personal Data Protection Authority, established by Law 675/1996.
- **Lottomatica Group**, is any company controlled and/or owned even indirectly by Lottomatica Group S.p.A.
- **People authorised to perform data processing**, the natural persons authorised by the Data Controller or Data Processor to carry out processing operations;
- **Data Subject**, the identified or identifiable natural person;
- **ITS**, Gamenet SpA's IT Security Department;
- **LCA**, Gamenet SpA's Legal & Corporate Affairs Department;
- **REG**, the Regulatory Compliance. AML & Quality Department;
- **TEO**, the Technology & Operations Department;
- **HRO**, the Human Resources & Organisation Department;
- **INA**, the Audit & GRC Department;
- **Security Measures**, the technical and organisational measures taken by the Data Controller to ensure and prove that the processing is carried out in accordance with the applicable legislation;
- **Processing activities register**, the register, kept by each Data Controller and/or Data Processor, of any processing activities carried out under their responsibility or, in the case of a Data Processor, of activities carried out on behalf of a Data Controller;
- **Contact Persons**, individuals within the Data Controller's structure who are in charge of one or more corporate functions that include one or more persons authorised to process personal data and who, as such, are selected and appointed by the Data Controller, on the basis of the principle of accountability referred to in section 1.1 of this procedure, to perform certain specific monitoring, verification, coordination and contact activities relating to the personal data processing activities for which they are responsible;
- **Data Processor** or **External Data Processor**, the natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller;
- **Data Controller**, the natural or legal person, public authority, service or other body that, individually or together with others, determines the personal data processing purposes and means;
- **Processing**, any operation or set of operations performed on personal data or sets of personal data, whether or not by automatic means, such as collecting, recording, organising, structuring, storing, adapting or modifying, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, comparing or interconnecting, limiting, erasing or destroying;
- **DPO** or **Data Protection Officer**, the Data Protection Officer referred to in Article 37 of the GDPR (see section 10 of this procedure);
- **Union**, the European Union.

Reference legislation:

- General Data Protection Regulation (GDPR-EU Regulation 2016/679) published in the European Official Journal on 4 May 2016 and entered into force on 25 May of the same year, effective in the member states of the European Union as of 25 May 2018.
- Guidelines and other documentation published by the Group of European Union Supervisors (so-called "WP29") pursuant to Article 29 of EU Directive 95/46.
- Personal Data Protection Code (commonly known as the Privacy Code), Legislative Decree 196 of 30 June 2003, as amended, where applicable;
- The measures and precautions required from data Controllers for processing carried out by electronic means in relation to the powers of system administrators, issued by the Italian Data Protection Authority on 27 November 2008, amended on the basis of the provision of 25 June 2009, where applicable.

Attachments:

The Attachments to this procedure form an integral and substantial part thereof:

a) Operating instructions on keeping the register of processing activities and data protection impact assessments and prior consultation;
b) Operational instructions concerning the notification of personal data breaches to the Supervisory Authority (so-called data breach).

Related Documents:

- Operating instructions for the processing of personal data
- Procedure on the correct use of corporate IT assets;
- IT asset life cycle management procedure;
- Data Backup and Recovery Management Procedure;
- Physical Access Management Procedure;
- procedure for processing data acquired through video surveillance systems;
- Passwords in sealed envelopes;
- Event logging and log access requests;
- Guidelines for the use of public and hybrid cloud systems;
- Data Cancellation Management Procedure;
- Data Breach Management & Notification Operating Procedure;
- Portability Management Operating Procedure.

5.4 ROLES AND RESPONSIBILITIES

The roles and responsibilities of the corporate functions and other stakeholders with regard to the protection of personal data are set out below.

Please refer to the following sections to define the operational methods to be adopted:

- Rules for processing without electronic means;
- Rules for processing by electronic means;
- Other organisational rules.

Data Controllers
Data controllers are those who determine the data processing purposes and means and are legally responsible for complying with the obligations provided for by the personal data protection legislation.

With reference to the Lottomatica Group, the Data Controllers can be traced back to each of the Group Companies, as legal entity, for the processing operations under their respective competence.

Data Processors
The GDPR identifies the data controller as the natural or legal person who processes personal data on behalf of the controller.

For the Lottomatica Group, the Data Processors are the following subjects:

- third-party suppliers on whom the Group relies for the processing of personal data;
- Gamenet S.p.A., as part of the provision of intra-group services, when these involve the processing of personal data.

The GDPR requires the data controller to provide sufficient guarantees to implement appropriate technical and organisational measures with respect to the requirements defined in the GDPR.

For this purpose, the Lottomatica Group undertakes to assess the adequacy of the Data Processors with respect to the above requirements and contractually regulates the terms and conditions relating to the processing of the personal data entrusted.

Contact people
Contact Persons are persons within the Data Controller's structure who are responsible for one or more corporate Functions that include within them one or more persons authorised to process personal data and who, as such, are selected and appointed by the Data Controller (on the basis of a logic of coherence of the overall corporate organisational model and its evolution) to carry out some specific activities of monitoring, verification, coordination and contact in relation to the personal data processing activities for which they are responsible, as well as to the effective implementation and continuous compliance with the technical and organisational security measures adopted by the Data Controller. Within the Lottomatica Group, all the front lines of Lottomatica Group S.p.A. have been appointed as Contact Persons within the scope of the functions assigned to them.

People authorised to perform data processing
Employees, interns and collaborators with employment contracts, consultants of external companies or independent collaborators, serving the Lottomatica Group are authorised to process the personal data necessary for the performance of the functions entrusted to them and to carry out only those processing operations that are instrumental thereto, also complying with the further instructions contained in this procedure, in related documents or given during the course of the activity and complying with the relevant provisions contained in specific internal communications.

For this purpose, it should be noted that the company's intranet contains operating instructions for data processing issued by the Lottomatica Group to all employees. The operating instructions may be consulted by all Group employees via the following path: "Documentation"> "Consult documents", "*Legal & Corporate Affairs" Area*> "Privacy". In any event, it is expressly understood that such instructions are in addition to any further instructions that may be published on the company's intranet or issued by one or more Lottomatica Group's Data Controllers on account of the specific task or particular processing assigned to each employee.

Moreover, in order to guarantee the correctness of the processing activities carried out by employees, the Lottomatica Group provides specific training initiatives for them.

With particular reference to health-related data and the special categories of data referred to in Article 9 GDPR of the employees of the companies of the Lottomatica Group and their family members, these may be processed by the staff of the following Departments: Human Resources & Organisation, Internal Audit & GRC and Legal and Corporate Affairs, as well as by the first-level department heads of the area in which the employee is employed and the employee's direct superiors.

System Administrators
System Administrators are professionals dedicated to the management of processing systems that process personal data, including database management systems, complex software systems (e.g. ERP), local networks and security equipment, to the extent that they enable them to act on personal data.

For the Lottomatica Group, the System Administrators include the employees of the Technology & Operations Area and those of external suppliers that provide processing system management services.

The requirements concerning the work of System Administrators are applicable until the date on which the legislation on the subject is still applicable (General Measure of the Italian Data Protection Authority on the "Measures and precautions to be adopted by data controllers when processing operations are carried out by electronic means with regard to the assignment of system administrator functions" of 27 November 2008, as amended by Measure of 25 June 2009).

The Lottomatica Group has adopted adequate measures to prevent and ascertain any improper use made by System Administrators through their privileges to access and manage systems and data. Roles and responsibilities relating to the adoption of such measures are described in the following sections.

Corporate & Legal Affairs Department
The Legal & Corporate Affairs function's data protection responsibilities cover the following main tasks:

- Definition and revision of the policies to be provided to the data subjects, in cooperation with the Data Protection officers identified within each Group company;
- Maintenance of the list of persons authorised to process data and their periodic training on data protection, in cooperation with the Human Resources & Organisation department;
- Keeping a list of data controllers and appointing them by written agreement; Definition of the format of letters for the appointment of system administrators;
- Drafting and sending responses to the exercise of data subjects' rights: access, rectification, cancellation, restriction, portability, opposition. With particular reference to the rights of erasure, restriction and portability, technical feasibility checks are carried out by the Technology & Operations and IT Security functions;
- Keeping of processing registers of the Lottomatica Group's Data Controllers and Processors, in cooperation with the Data Protection contact persons identified within each Group company;
- Keeping and updating the Data Breach Incident Register;
- Legal assistance in data protection impact assessments, in cooperation with the IT Security department;
- Analysing personal data breach reports and, if necessary, sending notifications to the Supervisory Authority, in cooperation with the IT Security department.

Internal Audit & GRC Department
- Conducting audits on the adequacy of business processes to the requirements of personal data processing legislation (European Regulation 2016/679 and implementing rules).

Human Resources & Organisation Department
- Identification and definition of organisational measures for the protection of personal data, in cooperation with the company departments involved in the areas for which they are responsible;
- Provision of the privacy policy to employees and other collaborators with atypical employment contracts at the beginning of the relationship, indicating the processing operations for which they are authorised;
- Assistance in maintaining the list of people authorised to process data and their periodic training on data protection, in cooperation with the Legal & Corporate Affairs department.

Technology & Operations Department
- Identification, definition and implementation of technical measures for the protection of personal data, in cooperation with the company departments involved in the areas for which they are responsible;
- Technical feasibility assessments of data subjects' requests for erasure, limitation and portability.

IT Security Department
- Identification, definition and implementation of technical measures for the protection of personal data, in cooperation with the company departments involved in the areas for which they are responsible;
- Technical feasibility assessments of data subjects' requests for erasure, limitation and portability;
- Maintenance of the digital register of system administrators and periodic verification of their work;
- Identification of the sphere of action of system administrators and definition of the same in the letters of appointment for these system administrators;
- Conducting data protection impact assessments, in cooperation with the Legal & Corporate Affairs department;
- Analysis of personal data breach reports, in cooperation with Legal & Corporate Affairs.

5.5 SECURITY MEASURES

Data security is defined on the basis of the following general principles:

- Confidentiality: ensuring that data is only accessible to duly authorised persons;
- Integrity: safeguarding the correctness and completeness of data, including by excluding unauthorised processing activities;
- Availability: ensuring that authorised persons have access to data when needed.

That being said, taking into account the existing technology and implementation costs, as well as the scope, purpose and objectives of the processing, as well as the risk of varying probability and severity for the rights and freedoms of individuals, Gamenet S.p.A., both in its capacity as data controller and data processor for the companies of the Lottomatica Group, implements adequate technical and organisational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate risk level, consideration must be given in particular to the risks presented by the processing resulting from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

5.6 RULES FOR PROCESSING WITHOUT ELECTRONIC MEANS

5.6.1 STORAGE OF DEEDS AND DOCUMENTS AND KEEPING OF ARCHIVES

Acts and documents of any kind, with particular regard to those containing personal data falling into special (so-called "sensitive") and legal categories, must be processed diligently, kept and stored in such a way that unauthorised persons cannot become aware of them. The acts and documents containing personal data must in any case be kept in archives that always allow, in the event of searches, access to the data on the basis of previously defined processing authorisations. Therefore, they must be filed by means of folders, classifiers, index cards or other containers, sorted according to uniform categories and based on criteria that enable them to be found according to specific search parameters that avoid consulting data that are not relevant to the task at hand.

Persons authorised to process data coming from (or directly taken from) selected-access archives must keep and safeguard the processed data with the utmost confidentiality, avoiding that they are voluntarily or involuntarily known by persons not having the same qualification as authorised persons to process data or who have assignments of a different scope. Access to the archives containing acts and documents containing personal data of any kind (identification data, data belonging to special categories ("sensitive") and legal data) is restricted to persons authorised to have access to them.

Only persons authorised to carry out activities in these areas, under a general authorisation covering all persons operating with the qualification of person authorised to process data, may access the archives of the individual company departments, limited to the company sectors to which they are normally assigned. Non-computer media containing the reproduction of information relating to the processing of sensitive and legal personal data or Gamenet's personal data must be kept and stored in the same way as provided for in this procedure, for the processing of original acts and documents.

5.6.2 ACCESS TO DATA

When any processing of personal data, recorded on paper or other non-computerised supports, is performed, the individual persons authorised to process the data must ensure that the processing operations are carried out only on the personal data for which knowledge is strictly necessary to perform the tasks envisaged for the specific activities attributed to the position held. Any processing of personal data that is not relevant to the company's professional purposes is accordingly prohibited. The archives of acts and documents containing personal data are accessed according to the specific instructions given by the department manager and are subject to the latter's control. Persons accessing files containing sensitive and legal data or personal data after closing time must be previously identified, authorised and registered.

5.6.3 DESTRUCTION OF PAPER DOCUMENTS

If documents containing personal data of any kind are to be disposed of for destruction, the person authorised to process the data must ensure that the data in question cannot come to the knowledge of persons who do not have the same qualifications (such as the external personnel involved in the destruction operations) by preparing them in an appropriate manner. Therefore, before being sent for shredding, documents consisting of single sheets of paper,

i.e. with a limited number of pages, must be destroyed individually, while documents with a greater number of pages, i.e. printouts resulting from automated processing, must be packaged (placed in boxes closed with adhesive tape and marked "confidential shredding" on the outside of the box) to guarantee their confidentiality for the subsequent shredding process carried out by the personnel in charge of this task.

5.7 RULES FOR PROCESSING WITH ELECTRONIC MEANS

For the rules on processing with the aid of electronic instruments, see the related procedures as mentioned in Article 3 of this procedure.

5.8 OTHER ORGANISATIONAL RULES

5.8.1 RULES ON PERSONS AUTHORISED TO PROCESS

- The HRO department notifies the recruitment of employees or other collaborators with atypical employment contracts by sending the name and department to the following address **dpo@lottomatica.com**. When the employment/collaboration relationship begins, the HRO department provides the person with information on the processing operations carried out by the employing company, which specifies that, when the employment/collaboration relationship begins and until it ceases or the Data Controller indicates otherwise, the person is authorised to process the data held by the Lottomatica Group within the limits of the processing operations relating to the department to which he/she belongs, as identified in the Processing Activities Register;
- Periodically, LCA holds a training course for all new recruits on the Regulation and the main security measures in force at Lottomatica Group;
- Whenever the working/collaboration relationship ends, the HRO department reports the event to the mailing list **dpo@lottomatica.com.**

5.8.2 RULES RELATING TO SYSTEM ADMINISTRATORS

- The System Administrator position is assigned after assessing the experience, capacity and reliability of the person to be appointed, who, in turn, must provide an appropriate guarantee of full compliance with the provisions in force on data processing, including the security profile (see paragraph 2, a) of the Supervisory Authority Order of 27 November 2008);
- The Human Resources & Organisation Department and the Department Manager to whom the person to be appointed is assigned conduct the assessment at the recruitment stage;
- Upon request by the IT function, the IT department issues a letter of appointment to each natural person assigned the role of System Administrator, which lists the areas of operation according to the authorisation profiles assigned;
- Whenever the functions of an already designated Internal System Administrator need to be integrated, the Department Manager to whom the person is assigned submits a request to the IT Security Department for a letter integrating the appointment;
- If the System Administrators' activity also indirectly concerns services or systems that process or allow the processing of workers' personal information, the Lottomatica Group's Data Controllers are required to disclose or make the identity of the System Administrators known within their organisations, depending on the features of the company or service, and in relation to the various IT services for which they are responsible;
- Where System Administration services are outsourced, the external processor must directly and specifically keep the identification details of the natural persons appointed as System Administrators, so that he/she can communicate them to the Data Controller should the latter so request;
- Appropriate systems must be adopted to record logical access (computer authentication) to processing systems and electronic files by system administrators. The records (access logs) must be complete, unalterable and their integrity verifiable so as to fulfil the purpose for which they are required. The logs must include time references and a description of the event that generated them and must be retained for a reasonable period, not less than six months;
- At least once a year, the System Administrators' activities must be subject to verification by the Data Controllers or Processors, where appointed, to check that they comply with the organisational, technical and security measures regarding the processing of personal data provided for by the rules in force. For this purpose, the IT S department checks the adequacy of the above organisational, technical and security measures every six months;

- The IT Security department is responsible for creating and maintaining the digital System Administrators Register, which identifies the most suitable technological instruments for management, storage and updating. The ITS department checks the list at least once a year.

5.9 INFORMATION TO PROVIDE THE DATA SUBJECTS

When adapting to the Regulation's provisions, the Lottomatica Group Companies have reformulated their privacy policies to meet the information obligations under Articles 13 and 14 of the Regulation.

Starting from 25 May 2018, all department managers who process personal data for the performance of their activities and the pursuit of objectives are required to consult Legal & Corporate Affairs in advance before starting any new or different processing of personal data, so as to verify with the LCA whether it is necessary to draft a new privacy policy or amend an existing one, and to inform the data subjects accordingly.

Personal data may not be processed by a business department until LCA has (i) issued the privacy policy to be provided to the data subjects and (ii) identified how the privacy policy is to be provided to the data subjects. The submission of the request for drafting/revision of the privacy policy and LCA's response thereto will be made by e-mail to ensure the traceability of the process.

In its response, LCA will indicate how the privacy policy should be provided to data subjects. Privacy policies should be dated and have an identification number (e.g. version 1.0).

The privacy policies must contain:

- the information elements referred to in Article 13 GDPR, if the data is obtained directly from the data subject;
- the information elements referred to in Article 14 GDPR, if the data is obtained from other sources. If it is not possible to inform the data subject of the origin of personal data, since several sources were used, general information should be provided.

If the Companies intend to process personal data for a purpose other than that for which it was collected, they must provide the data subject, prior to such further processing, with details of that other purpose and other necessary information. Therefore, department managers must consult LCA in writing before processing personal data for a purpose other than that for which it was collected.

Privacy policies may not be provided if and to the extent that the data subject already has the information.

5.10 THE DATA SUBJECTS' RIGHTS

The GDPR protects the data subject by reserving specific rights (Articles 15 et seq.) on their personal data. The deadline for replying to the data subject is, for all rights, one month, which can be extended up to three months only in cases of particular complexity. The data controller must in any case reply to the data subject within one month of the request, even in the event of refusal or of a particularly complex request (in the latter case, the data controller must inform the applicant that a complete reply will be provided within 3 months). As a general rule, the response must be in writing, including by electronic means that facilitate accessibility. The response must be concise, transparent and easily accessible.

The data subjects' rights can be exercised by sending an e-mail to the following address **dpo@lottomatica.com**.

Irrespective of the specific right exercised, in order to avoid undue requests, identical names or similar inconveniences, the data controller or processor shall verify the identity of the data subject by requesting him/her to submit or attach a copy of a valid identification document or by means of an authentication procedure. If the data subject is assisted by a third party, he/she must present or attach a copy of the power of attorney, together with a non-authenticated photocopy of the data subject's identification document. If the request is made on behalf of a legal person, the controller also requests a copy of the delegation of powers.

In particular, the data subject is entitled to the following rights:

- Right of access (Article 15): the data subject has the right to obtain from the data controller confirmation as to whether or not his or her data is being processed and to obtain access to his or her personal data. If

the request does not violate the rights and freedoms of others, the LCA department prepares the reply and provides a digital copy only of the personal data covered by the request, as extracted by the department authorised to process the data, specifying to the data subject that, in the event of further copies (including hard copies), the data controller may charge a fee for the administrative costs;

- Right to rectification (Article 16): the data subject has the right to obtain from the data controller the rectification of inaccurate personal data, as well as the integration of incomplete personal data. Once the request has been received, the LCA department will forward it to the competent department so that the latter can promptly proceed with the rectification/supplementation. Once evidence of the processing of the request has been obtained-which in any case must take place within and no later than 15 (fifteen) days from submission-the LCA department will send the data subject confirmation of the rectification/supplementation. Furthermore, the Purchasing & Shared Services department will notify each supplier to whom the personal data of the data subject have been communicated about the rectification.
- Right to erasure (Article 17): The data subject has the right to obtain from the data controller the erasure of personal data if: (i) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; (ii) the data subject withdraws consent; (iii) the data subject objects to the processing and there is no overriding legitimate reason to proceed with the processing; (iv) the personal data is unlawfully processed; (v) the personal data must be erased to comply with a legal obligation. For further details, please refer to the Data Cancellation Management procedure.
- Right to restriction of processing (Article 18): the data subject has the right to obtain from the data controller the restriction of processing when one of the following cases occurs: (i) the data subject contests the accuracy of the personal data, for the period necessary for the controller to verify the accuracy of the personal data; (ii) the processing is unlawful and the data subject objects to the erasure of the personal data and requests the restriction of their use; (iii) the controller no longer needs the personal data for processing purposes, the personal data is necessary for the establishment, exercise or defence of a legal claim; (iv) the data subject has objected to the processing, pending verification as to whether the legitimate reasons of the controller prevail over those of the data subject. With the exception of storage, any further processing of the data for which restriction is requested is prohibited unless certain circumstances are met (consent of the data subject, establishment of legal claims, protection of the rights of another natural or legal person, relevant public interest). After checking the requisites for the exercise of the right by the data subject, the LCA department informs the IT Security and Technology & Operations department of the request. Once the activity is completed, the IT Security department, within and no later than 15 (fifteen) days, sends to the LCA department the confirmation of the adoption of the necessary measures and the latter proceeds to reply to the data subject's request. Furthermore, the Purchasing & Shared Services department shall inform each supplier to whom the data of the interested party have been communicated of the cancellation/rectification.
- Right to data portability (Article 20): the data subject has the right to receive his or her personal data provided to a controller in a structured, commonly used and machine-readable format and has the right to have such data provided to another data controller without impediment by the controller to whom he or she has provided the data if: (i) processing is based on consent for one or more specific purposes, whether it concerns identification data, special categories of data pursuant to Section 9 or a contract; (ii) processing is carried out by automated means. In exercising his or her rights, the data subject has the right to obtain the direct transfer of data from one data controller to another if technically feasible. The right to portability must not infringe the rights and freedoms of others. For further details, please refer to the Portability Management operational procedure.
- Right to Object (Article 21): the data subject has the right to object at any time to the processing of his or her personal data, including profiling. The controller refrains from further processing the personal data unless the controller demonstrates the existence of compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims. If personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of his or her personal data for such purposes, including profiling where it is related to the direct marketing. After checking that the requirements for the exercise of the right by the data subject are met, the LCA department informs the IT Security and Technology & Operations department of the request. Once the activity is completed, the IT Security department, within and no later than 15 (fifteen) days, sends to the LCA department confirmation of the adoption of the necessary measures and the latter proceeds to meet the data subject's request.

5.11 DATA PROTECTION OFFICER

The Data Protection Officer (DPO) is an organisational entity appointed by the Data Controller to assist in all matters concerning the protection of personal data. The DPO must be designated based on his or her professional qualities

and in particular his or her specialist knowledge of data protection legislation and practices (national and European), as well as his or her ability to fulfil the tasks for which he or she is responsible (see, in particular, Article 39 GDPR). The DPO operates in complete autonomy and does not receive any instructions for the performance of duties from the Data Controller.

The DPO's tasks include:

- **(i)** the duty to keep updated on the current legislation and on the interpretations provided by the national and European Guarantor and to carry out periodic training courses for authorised data processors;
- **(ii)** the duty to monitor compliance with the GDPR and any other applicable data protection provisions;
- **(iii)** At the request of the controller, processors or those authorised to perform data processing, the DOP must provide advice on the obligations and compliance with current legislation, pursuant to the GDPR and the privacy legislation
- **(iv)** The DPO is a contact point for the Guarantor and the Authorities, as well as for data subjects. Cooperating with the Authorities also falls within the DPO's duties.

This procedure informs all employees that the companies of the Lottomatica Group have deemed it appropriate to appoint a DPO. The DPO can be contacted at the following e-mail address for any information or need related to the protection of personal data processed by the Lottomatica Group companies: **dpo@lottomatica.com**.

5.12 TRANSFERS OF PERSONAL DATA TO COUNTRIES OUTSIDE THE EUROPEAN UNION

Any transfer of personal data processed or intended to be processed after transfer to countries outside the European Union or to international organisations is allowed when these countries ensure the data protection adequacy standards listed in the Regulation.

If no adequacy is recognised, data controllers may use specific contractual safeguards for the transfer, for which the GDPR provides detailed and binding rules.

In the absence of contractual guarantees or acknowledgements of adequacy, data may only be transferred with the explicit consent of the data subject, or when special conditions are met (e.g. when the transfer is essential to comply with specific contractual obligations).

The Group guarantees the data subjects' right to obtain information on the recipients or categories of recipients to whom the personal data have been or will be disclosed, by submitting a request via e-mail or regular mail.

5.13 PERIODIC CHECKS AND INSPECTIONS

Apart from the independent audits that may be conducted by the Internal Audit & GRC department, the Data Controller and the Data Processor may arrange for periodic checks and inspections on the punctual compliance with the provisions of the GDPR; moreover, they will verify, at least once a year, the work of the System Administrators, to check that it is compliant with the organisational, technical and security measures regarding the processing of personal data provided for by the regulations in force. Without prejudice to the foregoing, at least once a year the Lottomatica Group reviews, also through its System Administrators, the users and data access authorisations on its systems.

6. DATA BREACH MANAGEMENT & NOTIFICATION

6.1 INTRODUCTION

The new European Regulation 679/2016 on the protection of personal data (hereinafter: GDPR) has extended, with Articles 33 and 34, the scope of the European Regulation 611/2013 on the obligation to communicate personal data breaches (so-called Data Breach) to the Supervisory Authority (unless the personal data breach is unlikely to present a risk for the rights and freedoms of natural persons) and, if the risk is high for their rights and freedoms, to the Data Subjects involved. This requirement, previously intended only for providers of electronic communication services, now involves all entities, Data Controllers, that fall within the material and territorial scope of the GDPR (Articles 2 and 3).

6.2 PURPOSE OF THE DOCUMENT

The purpose of this document is to describe the methods for managing information security incidents that constitute a personal data breach, for preparing notification to the Control Authority and, where necessary, to the Data Subjects involved, in compliance with the criteria, methods and time frames provided for by the aforementioned legislation.

With reference to the management of logical security events, the "Data Breach Management and Notification" procedure is implemented at the same time as the " Information Security Incident Management" procedure, which is under the responsibility of the IT department, both in the event of detection of anomalies on the systems through continuous monitoring and reports received from employees and external parties (e.g. partners, suppliers, etc.).

6.3 SCOPE

This procedure is applied within the Lottomatica Group.

6.4 DEFINITIONS AND ACRONYMS

Abbreviations	Meaning
D. Lgs.	Legislative Degree

Abbreviations	Meaning
ENISA	European Network and Information Security Agency
Data Breach	"Security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed" (Article 4, paragraph 1, No. 12 of the GDPR)
Processing	"any operation or set of operations which are performed on personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or interconnection, restriction, erasure or destruction;" (Article 4, paragraph 1, No. 2 of the GDPR)

Data Controller	"The natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria applicable to nomination of the controller may be determined by Union or Member State law" (Article 4, paragraph 1, No. 7 of the GDPR)
Data subject	"The natural person identified or likely to be identified to whom the personal data relate, e.g. a customer, prospect, employee or supplier"

Abbreviations	Meaning
Personal Data	"Any information relating to an identified or likely to be identified natural person, a data subject; an identifiable person is one who can be identified, directly or indirectly, by reference to, in particular, an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity" (Article 4, paragraph 1, No 1 of the GDPR)
Lottomatica Group	Lottomatica S.p.A. and/or other companies subject to the management and coordination of Lottomatica Group S.p.A.

CLA: Corporate & Legal Affairs

ITS: IT Security

IT: Information Technology

TEO: Technology & Operations

REG: Regulatory Compliance, AML & Quality

DPO: Data Protection Officer

6.5 RESPONSIBILITIES

Below is a summary table identifying, for each person involved in the process described, the responsibilities arising from this document.

Subjects involved	Responsibilities
IT	• Detecting the incident through monitoring of systems • Inform Corporate & Legal Affairs
DPO	• Assessment of the severity of the Breach and the need to notify the Data Subjects of the Breach • Prepare and send the Notification to the Privacy Guarantor and to the Data Subjects
CORPORATE & LEGAL AFFAIRS	• Assess the security incident • Request any additional information on the Data Breach from the internal/external bodies involved • Inform the DPO • Prepare and send the Notification to the Data Subjects

EXTERNAL DATA PROCESSOR	• Detect and report incidents out of the scope monitored by IT • Provide any additional information on Data Breach requested by Corporate & Legal Affairs
OTHER DATA CONTROLLER	• Receipt of Security Event Notification in the event of Breach of data not under the control of the Lottomatica Group

6.6 TYPE OF PERSONAL DATA BREACHES AND EVENT IMPORTANCE

a) TYPE OF PERSONAL DATA BREACHES

Based on the ENISA (European Network and Information Security Agency) Guidelines, security incidents that can be configured as personal data breaches (hereinafter referred to as data breaches) have been classified into six types:

- **Unauthorised Access:** access to personal data by persons (internal or external) who are not entitled to access;
- **Loss:** temporary unavailability of data;
- **Destruction:** irreversible unavailability of the data;
- **Transmission:** communication (accidental or intentional) of the data to unauthorised recipients;
- **Alteration or Modification:** improper modification (accidental or intentional) of data;
- **Disclosure:** improper disclosure of confidential information.

b) EVENT IMPORTANCE

The following is a list, by way of example and in any event not in any way exclusive, of the possible events that could cause the personal data breaches specified above. However, the occurrence of one of the events described below does not constitute a sufficient condition for establishing a Data Breach, as the conditions set out in Articles 33 and 34 of the GDPR must be met.

ACCIDENTAL EVENTS

Unusual events caused by accidental circumstances leading to the loss of data subjects' personal data security features (confidentiality, integrity, availability or resilience of the systems) in the case of automated processing carried out by computer systems or non-automated processing by means of paper files, such as:

- **Incorrect execution of commands and/or procedures due to distraction:** e.g. erroneous publication of personal information (not in the public domain) on public web portals, erroneous sending of information to entities outside the Lottomatica Group, formatting of storage devices, errors in the implementation of a control policy and periodic verification of access authorisations; accidental disclosure of access credentials to colleagues or unauthorised personnel, etc.;
- **Breakdown of hardware components:** e.g. destruction of storage media due to changes in temperature and electricity, humidity, short circuit, accidental loss, catastrophic events/fire, etc.;
- **Software Malfunctioning:** execution of an unauthorised automatic script, programming errors that lead to incorrect **outputs**, etc.;
- **Submission of incorrect data on the Reserved Area: visibility** by customers of other customers' data, also due to identical names, etc.;
- **Disclosure of data to a person other than the data subject:** by way of example, communication of customer data to incorrect recipients, management and processing of complaints/information requests made by persons other than the Data Controller, sending/displaying of invoices to persons other than the Data Subject;
- **Loss of documents:** loss of documents containing data of customers or other Data Subjects by business partners (e.g. providers of document archiving services), etc.;
- **Loss of corporate assets:** accidental loss of storage and/or processing media containing Data Subjects' personal data (e.g. laptops, hard disks, USB sticks, smartphones, tablets, etc.);
- **Accidental destruction of documents:** fire/ flooding of the premises where paper archives are located, caused by accidental and non-malicious events at the premises of the Lottomatica Group and of commercial partners (e.g. suppliers of document archiving services); accidental destruction of original documents, without any copies, by internal employees, commercial partners, etc.

MALICIOUS EVENTS

Malicious events caused by internal staff or external parties carried out through:

- **Unauthorised access** to personal data by exploiting vulnerabilities in internal systems and communication networks;
- **Unlawful interference with or disclosure** of authentication credentials;
- **Use of malware.** This includes security incidents involving the violation of personal data of customers or other data subjects, such as:
  - **Theft:** theft of storage and/or processing media containing personal data (e.g. laptops, hard disks, USB sticks, smartphones, tablets, etc.);
  - **External computer fraud:** all cases of fraud committed by a person external to the company for the purpose of obtaining for himself or others a profit or, in any case, an advantage in economic, advertising, ideological/political terms, which causes loss of the data security features of the data subjects' personal data (confidentiality, integrity or availability) processed by the Lottomatica Group or its suppliers (e.g. unauthorised and unlawful access to systems containing customer data by exploiting vulnerabilities in the same systems; appropriation of credit card data; appropriation and possible dissemination of authentication credentials for customer services, etc.);
  - **In-house computer fraud:** all cases of fraud carried out by personnel within the company involving the violation of personal data. Such events may result from the unlawful and/or illegitimate use of information accessed by a person in charge of processing personal data, even if authorised. Data breaches do not include cases where there is no loss of confidentiality, integrity or availability of the data subjects' data (e.g. fictitious registration of contracts with unsuspecting customers, which is a case of commercial fraud).

6.7 DETECTION AND ANALYSES

a) SECURITY INCIDENT DETECTION AND ASSESSMENT

Security events that could constitute a data breach can be detected both internally by:

- IT, through recursive control and monitoring activities on internal applications and systems;
- Contacts identified within the Lottomatica Group units and areas, through reports from internal (e.g. employees) or external (e.g. customers) sources;
- or externally by:
- Suppliers, appointed as External Data Controllers, through recurring control and monitoring activities on:
  - Lottomatica Group's applications and systems (in the case, for example, of IT suppliers) or its applications and systems involved in the Lottomatica Group's personal data processing;
  - processing carried out on behalf of the Lottomatica Group without the use of electronic tools (e.g. paper filing).

In particular, events detected internally through continuous monitoring of the systems supervised by IT or reported by the corporate areas (both business and staff) and external to the computer area supervised by IT (e.g. incident relating to a paper archive, loss or theft of a corporate asset), or detected by the External Data Processors, are reported to **databreach@lottomatica.com**, through ordinary corporate communication channels (e.g. e-mail, telephone).

Upon detecting a security incident or receiving a report from internal or external sources, Corporate & Legal Affairs, with the support of IT SEC:

a) if the security event relates to data not belonging to the Lottomatica group, but which it handles in its capacity as External Data Processor, it will forward the Security Incident notification to the Principal within 24 hours of becoming aware of it;

b) if the incident relates to data pertaining to the Lottomatica Group, together with IT SEC, it shall analyse the event, determining whether it constitutes a Data Breach and assessing the relative risk level and its potential impact. The output of this activity can be of two types:

- The security incident takes the form of a data breach;
- The security incident does not involve personal data.

b) COLLECTION OF INFORMATION RELATIVE TO THE DATA BREACH

Following the analysis of the event, Corporate & Legal Affairs and IT SEC will:

a) Request any further information that may be necessary, in the event of a data breach, involving, depending on the case:

- Contact person of the business unit or area that detected the incident;
- External Data Processor from whom the report was received;
- IT, if the detection of the incident occurred through control and monitoring activities on Lottomatica group systems.

b) File the security event as a false alarm in a special register (so-called Data Breach Register), if it was assessed as a simple Information Security Incident, in respect of which the "Information Security Incident Management" procedure remains applicable.

INVOLVEMENT OF THE DPO

Having collected all the necessary information and any supporting documentation, Corporate & Legal Affairs involves the Data Protection Officer (hereinafter DPO) who analyses the Data Breach and decides on appropriate recovery actions with the various corporate departments involved.

6.8 INFORMING THE ITALIAN DATA PROTECTION AUTHORITY OF THE DATA BREACH

Based on Article 33 of the GDPR, if there is a data breach of the Data Subjects' personal data, the Data Controller will inform the Italian Data Protection Authority of the breach promptly and, where possible, within 72 hours of becoming aware of it, unless the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons.

a) **PREPARING THE NOTIFICATION**

Together with Corporate & Legal Affairs and the IT SEC, the DPO prepares the Data Breach Notification using the template available on the Italian Data Protection Authority's website, "Data Breach Notification Template", which must contain, as a minimum, the information listed below:

- the nature of the personal data breach including, where possible, the categories and number of data subjects and the types and approximate number of personal data records involved;
- the DPO's name and contact details and any contact points that may provide further information deemed useful by the Authority;
- the likely consequences in terms of the impact of the personal data breach;
- the remedial measures and actions adopted or envisaged by the Data Controller, deemed appropriate to mitigate possible impacts on the rights and freedoms of the Data Subjects.

b) **SENDING AND FILING OF THE NOTIFICATION**

No later than 72 days after the Data Controller becomes aware of the breach, the DPO sends the Notification to the Data Protection Authority. At the same time, Corporate & Legal Affairs files the information contained in the Notification to the Italian Data Protection Authority in the appropriate Data Breach Register, which is created and maintained in accordance with the Authority's Guidelines (completeness, integrity and non-changeability of records).

6.9 INFORMING THE DATA SUBJECTS OF THE DATA BREACH

According to Article 34 of the GDPR, when the personal data breach is likely to present a high risk to the rights and freedoms of natural persons, the Data Controller must also notify the Data Subject of the Data Breach promptly, unless it can demonstrate to the Italian Data Protection Authority that it has adopted:

- Prior to the breach, appropriate technical and organisational measures, in particular those designed to make personal data indecipherable to anyone not authorised to access it, e.g. encryption (Article 34, paragraph 3, letter a of the GDPR);
- Following the breach, measures to prevent the emergence of a high risk to the rights and freedoms of the data subjects (Article 34, paragraph 3, letter b of the GDPR);

In any event, breaches of authentication credentials (i.e. Username and Password) and encryption keys used by the Data Subjects must always be communicated to them.

6.10 ASSESSMENT OF THE IMPACTS ON THE DATA SUBJECTS

The DPO assesses the risks and related impacts of the personal data breach on the individuals concerned, in order to determine whether the risk is so high that it is necessary to notify the Data Subjects as well.

a) **PREPARING THE NOTIFICATION**
The DPO finds the list of the data subjects involved in the breach, if necessary, requesting further information from both internal contact persons and External Data Processors.
The Notification to Data Subjects must contain at least the same information as that communicated to the Italian Data Protection Authority regarding impacts, the security measures taken and the contact details of the DPO.

b) **SENDING AND FILING OF THE NOTIFICATION**
After preparing the Notification, the most effective communication channel to reach all the persons involved is identified and sent to the Data Subjects without undue delay. At the same time, Corporate & Legal Affairs shall file the information contained in the Notification to Data Subjects in the Data Breach Register, which shall be created and maintained in accordance with the Authority's Guidelines (completeness, integrity and non-changeability of records).

6.11 MANAGEMENT OF THIRD PARTIES ENTRUSTED WITH THE PROVISION OF A SERVICE

The legal requirements relating to data breaches also cover cases where the Data Controller entrusts third parties with the provision of a service involving the processing of personal data. Article 33, paragraph 2 of the GDPR emphasizes that "The Data Processor must inform the Data Controller immediately after having become aware of the breach".

a) **REPORTING OF PERSONAL DATA BREACHES BY SUPPLIERS**
The requirements of Article 33 of the GDPR are regulated within the contracts and agreements entered into between the Lottomatica Group and third parties in a special section of the letter of Appointment as External Data Processor and the related Operating Instructions. These obligations must be complied with by the Lottomatica Group if it is appointed as External Data Processor by another Controller.

If a security incident occurs in connection with the processing carried out on behalf of the Lottomatica Group for the purpose of providing the service covered by the order, or if the Lottomatica Group carries out such processing in its capacity as Processor, the supplier performs an initial analysis of the event and sends a report of the ascertained breach immediately. The report must contain all the elements useful for understanding/identifying the event. Specifically, it must provide at least the following information concerning the security event:

- Business name of the Data Processor (including any Sub-Processor involved) affected by the incident that may lead to a personal data breach;
- Date and time when the accident occurred;
- Nature of the incident that occurred;
- Categories and number of data subjects whose personal data were affected by the incident;
- Type and volume of personal data affected by the incident;
- Probable impacts and consequences of the incident;
- Measures put in place before and after the Data Breach to mitigate possible impacts on the rights and freedoms of Data Subjects.

The third party involved is also required to support the Lottomatica Group by providing any additional information required for the correct assessment and management of the security event.

7. DATA RETENTION MANAGEMENT

7.1 FOREWORD

The Lottomatica Group (i.e. Lottomatica Group S.p.A. and the companies controlled and/or owned also indirectly by it) issues the following procedure ("Procedure") with regard to the processing of personal data and the free movement thereof in accordance with European Regulation 2016/679 (hereinafter also "Regulation" or "GDPR"), in order to identify and indicate the rules for the preservation of documents and information (both paper and electronic) in full compliance with the current legislation and regulations in force, as well as with the general principles dictated by the Lottomatica Group.

Documents and information stored by Lottomatica Group companies represent an important corporate value and require appropriate and targeted management that preserves their value over time and protects the interests of the Group and stakeholders.

Taking into account the principles of storage limitation set forth in Art. 5 letter e), as well as the principle of data minimization set forth in Art. 5 letter c) of the Regulations, the Lottomatica Group intends to equip itself with this Procedure as a valuable tool to help define the terms of storage of documents and information (both paper and electronic) thus ensuring that:

- the retention time is proportional to the fulfillment of the purposes for which the personal data were collected;
- personal data for which the retention period has expired are deleted.

7.2 OBJECTIVE

This Procedure contains indications on the maximum retention times of documents and information kept by the companies of the Lottomatica Group, as part of their personal data processing activities.

In this sense, the Procedure serves as "Internal Regulations" in which the expected behaviors are made explicit in order to ensure that the storage of personal data takes place in compliance with the principles imposed by the GDPR.

7.3 ADDRESSEES

This procedure is applicable within the Lottomatica Group and is addressed to all divisions.

7.4 DEFINITIONS AND RELATED DOCUMENTS

The following terms and definitions shall have the meaning ascribed to each of them below, it being specified, however, that terms defined in the singular shall also be understood to be defined in the plural and vice versa. It being understood that additional terms, other than those defined herein, shall have the meaning ascribed to them in the GDPR and its implementing regulations. For the purposes of this procedure:

- **Personal Data:** any information concerning a Data Subject (Art. 4, c. 1, no. 1 of the GDPR);
- **Employee:** any individual (natural person) who performs his or her work activity in the employ of one of the companies of the Lottomatica Group (specifically designated as authorized to process);
- **Documents:** any document, information, data, whether paper, electronic (including e-mails, drafts and everything contained on company PCs or within the data center) or recorded on any other medium, regardless of place or physical form;
- **Data Subject:** the natural person to whom the Personal Data processed by the Data Controller relates and belongs;
- **Data Processor:** the natural or legal person, public authority, service or other body that processes Personal Data on behalf of the Data Controller (Articles 4(1)(8) and 28 of the GDPR);
- **Third Party:** any person involved in the business processes by virtue of a consulting contract and/or other type of contract;

- **Data Controller:** the natural or legal person, public authority, service or other body which, individually or jointly with others, determines the purposes and means of the Processing of Personal Data (Art. 4, c. 1, no. 7 of the GDPR);
- **Processing:** means any operation or set of operations, whether or not involving automated processes, applied to Personal Data or sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or interconnection, restriction, erasure or destruction (Art. 4, c. 1, no. 2 of the GDPR);
- **Office:** means one of the corporate functions part of the organizational structure of the Lottomatica Group.

Related documents:

- PA CLA 02 Data Protection Regulation Procedure;
- PA CLA 13 Procedure for Managing Access to Personal Data Contained in the Archives;
- IO TEO 04 Data Deletion-Reuse of ICT Resources.

7.5 REFERENCE LEGISLATION

The Procedure refers to the following legislation:

Title / description	Code
Regulation (UE) 679/2016 – GDPR	GDPR
General Provisions and guidelines of Privacy Authority as applicable	Provisions oh Privacy Authority
National Legislation - D.lgs 101/2018 modifying del D.lgs 196/2003	Privacy Code Civil Code

In order to compute the period of data retention and to make up for the shortcomings and regulatory gaps in this area, one of the criteria used is the analogical extension, apt to regulate equivalent and unregulated cases, applying rules provided for similar cases.

The time periods provided refer to both traditional and electronic documents.

The maximum time period indicated must be considered applicable to all documentation produced following the provision of Personal Data and stored in the relevant places (in the case of paper storage) or in the servers or computer tools (in the case of data on electronic support) to which only authorized personnel have access.

7.6 REFERENCE CONTEXT

Current legislation, especially the GDPR, the Privacy Code and the Privacy Guarantor Measures, govern the guiding principles for defining the terms of storage of Personal Data.

From a regulatory point of view, according to Article 5 of the GDPR, Personal Data subject to processing must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit, legitimate purposes, and used in other processing operations in terms compatible with those purposes;
- adequate, relevant, complete and not excessive in relation to the purposes for which they were collected or subsequently processed;
- accurate and, if necessary, updated;
- **kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which they were collected or subsequently processed:** Personal Data may be processed for longer periods provided that they are processed solely for archiving purposes in the public interest, scientific or historical research or statistical purposes, subject to the implementation of appropriate technical and

organizational measures required by the GDPR;
- processed in a manner that ensures adequate security of Personal Data, including protection, by appropriate technical and organizational measures, from unauthorized or unlawful processing and accidental loss, destruction or damage.

7.7 RETENTION PERIODS

The maximum retention period of Personal Data is inherently related to the purposes for which said Personal Data was obtained and stored.

The retention times of Personal Data are indicated in the treatment records of each company of the Lottomatica Group and can always be consulted on the company intranet, in the section Documents > Legal & Corporate Affairs >Privacy, by accessing through the following link: https://intranet-my.lottomatica.com/documenti/9/104/ .

It is in any case understood that the retention periods of the Data indicated in the registers may be extended in the event of the Data Controller's need to maintain the Data in order to exercise its rights in court, or in the event of requests by public and/or judicial authorities, and in any case in any hypothesis in which it is necessary for the purposes of the proper performance of the Processing.

7.8 CANCELLATION

Deletion of Data means the physical or technical destruction sufficient to render the information contained in a document no longer recoverable by ordinary commercially available means.

The Data Controller has adopted agreed and approved destruction methods by means of the operating instruction "IO TEO 04 Data Deletion-Reuse ICT Resources."

7.9 INTERNAL CONTROL SYSTEM

Employees, specially designated as authorized processors, depending on the Office to which they belong, are obliged to monitor compliance with the data retention criteria defined within the records, in order to:

(i) enable the rational management of paper and computer files,
(ii) verify that only the data actually needed are kept, and
(iii) ensure compliance with the regulatory references set forth in this Procedure.

7.10 REFERENCES AND AMENDMENTS

The contents of this Procedure shall be updated in cases of changes in regulations regarding the processing of personal data. For all matters not regulated by this Procedure, reference is made to the Laws in force, their implementing measures, the decisions of the Guarantor and any other legislation, special, general, national and EU regulations on the protection and processing of personal data in the context of the rights of the Interested Parties.

Insofar as it is compatible, this procedure must be read in conjunction with (and therefore supplemented by) the Internal Regulations adopted by the company to ensure the adaptation of the processing activities carried out by the personnel of the companies of the Lottomatica Group to the requirements and limits imposed by the GDPR and more generally by all current legislation on the protection of personal data of individuals.

8. INFORMATION TO SUPPLIERS AND/OR OTHER CONTRACTUAL PARTNERS

PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 GENERAL REGULATION ON DATA PROTECTION

We would like to inform you that EU Regulation 2016/679 (the "**Regulation**") and the relevant Italian legislation supplementing them establish rules on the protection of individuals with regard to the processing of personal data and protect the fundamental rights and freedoms of individuals, and in particular the right to the protection of personal data. Pursuant to articles 13 and 14 of the Regulation, we hereby inform you of the methods and purposes with which each contracting Lottomatica Group Company, as Data Controller, will process your personal data. Please read this privacy policy carefully before providing us with your personal data or, where requested, consenting to their processing. Please consider that this privacy policy concerns the processing of personal data of:

(i) suppliers and/or other contractual partners who are natural persons; and
(ii) legal representatives, partners (natural persons) and directors of suppliers and/or other contractual partners who are legal persons.

***

1. HOW DID YOU GET MY PERSONAL INFORMATION?

We collect your personal data directly from you when negotiating or concluding a contract or through databases of entities offering information on the commercial reliability of entrepreneurs and managers and/or on the possession of the required subject/reputation requirements (see paragraph 2.c below).

2. FOR WHAT PURPOSES WILL MY PERSONAL DATA BE PROCESSED?

We will process your personal data for the following purposes:

a) **To comply with legal obligations** (*art. 6, para. 1, letter c) of the Regulation*)
We will process your personal data in order to fulfil our obligations under current tax legislation. Furthermore, we will process your personal data in order to comply with the legal obligations provided for by the Italian legislation concerning the prevention of the use of the financial system for the purpose of laundering the proceeds of criminal activities and the financing of terrorism (Legislative Decree 231/2007), as well as to verify the possession of the subjective (reputational) requirements necessary for contracting with each of the Companies of the Lottomatica Group. To this end, we will collect a copy of your identity document and, in addition, we will consult certain databases of subjects that offer information on the commercial reliability of entrepreneurs and managers and/or the possession of the aforementioned reputational requisites, in order to obtain information relating to your commercial reliability and possession of the subjective requisites required. The data extracted from these databases belong to the following categories:
- economic-financial data;
- reputational data;
- data needed to carry out asset investigations.

b) **To execute a contract to which you are a party and pre-contractual measures adopted at your request** (*art. 6, paragraph 1, letter b) of the Regulation*)
We will process your personal data in order to execute each contract concluded between you and us or to execute pre-contractual measures taken at your request.

c) To pursue our legitimate interest in mitigating our commercial risk (*art. 6., para. 1, letter f) of the Regulatio))*
Before the conclusion of the contract and during its execution, we will process your personal data in order to assess your solvency and financial reliability. We will also consult certain databases of entities that provide information on the commercial reliability of entrepreneurs and managers in order to obtain information regarding your commercial reliability and the possession of the subjective (reputational) requirements necessary for contracting with each of the Companies of the Lottomatica Group. The data extracted from these databases belong to the following categories:

- economic and financial data;
- reputational data
- data needed to carry out asset investigations.

For more information on how these entities process your personal data, please consult the privacy policy of the National Association of Business Information Companies, published on the website **www.informativaprivacyancic.it**. The Company will process this data and information to pursue its legitimate interest in mitigating its business risk.

d) To pursue our legitimate interest in assessing your contractual diligence and your company's performance (*art. 6., para. 1, letter f) of the Regulation*)
While performing the contract, we will process your personal data, including those obtained from the commercial information systems and economic and financial soundness systems referred to in paragraph c) above, in order to pursue our legitimate interest in assessing your diligence in performing the contract and the commercial performance of your company, in order to assess whether and under what conditions to continue maintaining a business relationship with your company. To this end, we may carry out a profiling and assign you a rating/ scoring to summarise our assessment in this regard. In any case, no fully automated decision will be made by us on the basis of such assessment or rating.

e) To pursue our legitimate interest in efficiently managing our suppliers through the supplier register *(art. 6., para. 1, letter f) of the Regulation)*
We will enter your details in our supplier register, in order to pursue our interest in managing suppliers efficiently and avoiding having to carry out the necessary checks on the suitability and adequacy of each supplier each time.

f) To pursue our legitimate interest in exercising or defending a right in or out of court *(art. 6., para. 1, letter f) of the Regulation)*
We will process your personal data in order to pursue our legitimate interest in exercising or defending our rights in or out of court, including in the event of breach of the contract.

3. IS IT COMPULSORY OR OPTIONAL TO PROVIDE DATA?

The provision of personal data is optional but necessary, as failure to do so will make it impossible to enter into a contract with us and to execute it.

4. HOW WILL MY PERSONAL DATA BE PROCESSED AND FOR HOW LONG WILL IT BE STORED?

Your personal data will be processed with automated and non-automated tools. Specific security measures are taken to prevent data loss, unlawful or incorrect use and unauthorised access.

Your personal data will be stored for the following time:

- 10 years from the date of termination of the contract for the purposes of fulfilling the legal obligations provided for by Italian legislation concerning the prevention of the use of the financial system for the purpose of laundering the proceeds of criminal activity and the financing of terrorism (Legislative Decree 231/2007);
- 10 years from the date of termination of the contract for the purpose of fulfilling the legal obligations provided for by the Italian Civil Code and Tax Laws concerning the obligations to keep company documents, except for possible extensions due to events that alter the legal statute of limitations;
- 1 year if, as a result of the pre-contractual assessment procedure or verification of the requirements referred to

in point 2(b) and (c), we decide not to proceed with the conclusion of the contract;
- The data contained in the supplier list will be stored for the duration of the contractual relationship and until your company has indicated to us that it no longer wishes to be included in our supplier list.

5. WHO COULD HAVE ACCESS TO MY PERSONAL DATA?

Your personal data may be disclosed to our employees and associates who deal with the conclusion and execution of the contract, as well as to our employees and associates who deal with the fulfilment of legal obligations in tax matters. In addition, the following categories of subjects may become aware of your personal data, who, as data processors, provide us with services instrumental to the performance of our activities: suppliers of IT services; suppliers of management services; suppliers of administrative services; external professionals and consultants; Lottomatica group companies providing intra-group services; companies specialized in carrying out asset investigations, external auditors, if any.

6. WILL MY PERSONAL DATA BE DISCLOSED TO THIRD PARTIES?

Your data may be communicated to third parties belonging to the following categories:

- banks and payment institutions, to the extent necessary to make or receive payments in connection with the contract;
- the competent tax and fiscal authorities, to the extent required by law;
- to the authorities involved in various capacities in the prevention of money laundering and the fight against the financing of terrorism;
- the judicial authorities or the police, if we need to report a crime or in any case where necessary to pursue a legitimate interest of ours to exercise or defend a right in court;
- lawyers, where necessary to pursue a legitimate interest in exercising or defending a legal claim in or out of court.

7. WILL MY PERSONAL DATA BE TRANSFERRED OUTSIDE THE EUROPEAN ECONOMIC AREA?

No, your personal data will only be processed within the European Economic Area.

8. WHAT ARE MY RIGHTS?

You have the right to exercise at any time, free of charge and without formality, the following rights under articles 15 to 22 of the Regulation: the right to request access to your personal data (i.e. the right to obtain confirmation from us as to whether or not data concerning you is being processed and, if so, to obtain access to your personal data, receive a copy of it, and the information referred to in art. 15 of the Regulation); to correct it (i.e. the right to have inaccurate data concerning you corrected or incomplete data supplemented) or have it deleted (i.e. the right to have data concerning you deleted, if one of the reasons indicated in art. 17 of the Regulation apply); to limit its processing (i.e. the right to have your data marked in the cases indicated in art. 18 of the Regulation, in order to limit its processing in the future), as well as the right to data portability (i.e. the right, in the cases indicated in art. 20 of the Regulation, to receive from us, in a structured format, in common use and readable by automatic device, the data concerning you, as well as to transmit such data to another Data Controller without hindrance). You also have the right to revoke your consent at any time. The revocation of consent will not affect the lawfulness of processing based on consent before the revocation. We remind you that you always have the possibility to lodge a complaint with the Data Protection Authority (**www.garanteprivacy.it**) or to another supervisory authority of the Member State of the European Union in which you reside or work.

9. DOES THE REGULATION ALSO GIVE ME THE RIGHT TO OBJECT TO THE PROCESSING?

Yes, you have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you pursuant to art. 6(1)(e) or (f) of the Regulation, including profiling on the basis of these provisions. If your personal data is processed for direct marketing purposes, you have the right to object at any time to its processing for these purposes, including profiling to the extent that it is related to direct marketing.

10. HOW CAN I CONTACT YOU AND EXERCISE MY RIGHTS?

Requests to exercise your rights, as indicated above, may be made by email to the following address **dpo@lottomatica.com**.

11. HOW CAN I CONTACT YOUR DATA PROTECTION OFFICER?

The Data Protection Officer can be contacted by email at **dpo@lottomatica.com**.

9. INFORMATION TO THE EMPLOYEES AND COLLABORATORS

PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 (GENERAL REGULATION ON DATA PROTECTION)

We would like to inform you that EU Regulation 2016/679 (the "**Regulation**") and the relevant Italian legislation supplementing them establish rules on the protection of individuals with regard to the processing of personal data and protect the fundamental rights and freedoms of individuals, and in particular the right to the protection of personal data. Pursuant to articles 13 and 14 of the Regulation, we inform you below of the methods and purposes with which Lottomatica SpA, as well as another company of the Lottomatica Group (i.e. Lottomatica SpA and the companies controlled and/or owned directly or indirectly by Lottomatica Group SpA) as data controller or data processor, will process your personal data. Please read this privacy policy carefully before providing us with your personal data or, where requested, consenting to their processing. Please note that this privacy policy covers the processing of the personal data of employees, collaborators, interns and workers in any other capacity, as well as, in the cases specified in this policy, their family members.

***

1. HOW DID YOU GET MY PERSONAL INFORMATION?

We collect your personal data directly from you during the recruitment process or when concluding or fulfilling the employment contract. In the recruitment phase, we may also have received your personal data from third parties, such as recruitment agencies or head-hunters, including personal data, contact data, data relating to your education and professional experience, sensitive data relating to your membership of protected categories and any other data included in your curriculum vitae. During the course of the employment relationship, we may also obtain some of your personal data from public bodies (INPS, INAIL, Provincial Labour Directorate, Tax Agency), e.g. in relation to your social security position or illness status. We may also receive data concerning you from private parties who provide us with services instrumental to the use and management of company assets (for example, if you use a company car, we may receive data relating to the entry and exit of your car from the motorway network from the manager of the electronic toll systems) or who otherwise process data concerning you (for example, if you commit a traffic offence using a company car, we may receive from the competent authorities the assessment report concerning you). Other personal data are collected automatically, such as data on the day/time of your entry into and exit from the workplace collected through badges).

2. FOR WHAT PURPOSES WILL MY PERSONAL DATA BE PROCESSED?

We will process your personal data for the following purposes:

g) **To comply with legal obligations** (*art. 6, sec. 1, letter c) of the Regulations*)
We will process your personal data in order to fulfil or require the fulfilment of specific obligations or to perform specific tasks provided for by European Union legislation, laws, regulations or collective agreements, including company agreements, in particular for the purposes of establishing, managing and terminating employment relationships, as well as the recognition of benefits or the disbursement of contributions, the application of regulations on social security and assistance, including supplementary ones, or on hygiene and safety at work or in the population, as well as on tax, trade union, health protection, public order and safety and the administrative liability of legal persons and companies.

h) **To perform a contract to which you are a party, along with any pre-contractual measures you request** (*art. 6, sec.1, let. b) of the Regulation*)
We will process your personal data in order to fulfil your contract of employment and manage your relationship

with us, to keep your accounts or to provide you with salaries, allowances, bonuses, other emoluments, gratuities or fringe benefits (for example, if you are given a company car). We may also process personal data concerning you prior to the establishment of the employment relationship in order to carry out any pre-contractual measures at your request.

i) **To pursue our legitimate interest in exercising or defending a right in or out of court** (*art. 6., sec. 1, let. f) of the Regulations*)
We will process your personal data in order to pursue our legitimate interest in exercising or defending one of our rights in judicial or extrajudicial proceedings, as well as in administrative proceedings or in arbitration and conciliation procedures in the cases provided for by laws, Italian and European Union legislation, regulations or collective agreements, including in the event of breach of contract or breach of law. Moreover, with specific reference to the processing carried out in relation to the use of electronic mail, the Internet and other technological resources, we may process your personal data, even after termination of the employment relationship, in order to ascertain whether any unlawful acts and/or behaviour damaging to the company's image or assets have been committed (see in this regard the specific procedure published on the company intranet "Guidelines for the correct use of IT resources").

j) **On the basis of your consent to the processing of your personal data for one or more specific purposes** (*art. 6., sec. 1, let. a) of the Regulation*)
In some circumstances, such as, for example, in the event that we have to publish your photo on your company ID card or on the company intranet, as well as in the event that we have to propose that you take part in voluntary company recreational initiatives, conventions, training courses, webinars organized by Lottomatica S.p.A. or by any other company in the Lottomatica Group and we decide to film you during said events (which may take place in person or with the use of telematic tools that allow remote participation), and/or publish such filming on the company intranet and/or on the platforms created for this purpose within the company intranet and/or on our social pages (Linkedin, Lottomatica Group's website), we shall process, subject to your optional consent, your personal data (images), it being understood that if you do not give your consent you will not suffer any prejudicial consequences.

k) **the processing is necessary to protect your vital interests** (*art. 6., sec. 1, let. d) of the Regulation*)
In the event of an emergency, such as an accident at work, we will process your personal data to safeguard your vital interests and enable you to receive help and assistance.

With your consent, we may also process the personal data of your family members - for example, if you ask us to take advantage of special benefits granted by law or company policy that are related to the status of your family members or directly available to your family members. We will also process the data of your family members if you wish to give us their contact details in case of emergency, to protect your vital interests. Please also provide a copy of this privacy policy to your family members. Unless the processing of your family members' data is required to comply with legal obligations, we will ask you to have your family members sign a declaration of informed consent to the processing.

For information on the processing and controls carried out in relation to the use of electronic mail, the Internet and other technological resources, please read the specific procedure published on the company intranet ("*Guidelines for the correct use of IT resources*").

Please also read the supplementary information regarding the data processed in connection with the use of our video surveillance systems attached hereto as Annex 1 ("*Video Surveillance*").

Finally, please consider that our company has implemented an organisation and management model pursuant to Legislative Decree no. 231/2001 aimed at preventing the criminal liability of companies, as well as a company procedure pursuant to Law no. 179/2017 to encourage the cooperation of workers in reporting within companies corrupt phenomena and other crimes relevant for the purposes of Legislative Decree no. 231/2001 (so-called *Whistleblowing* procedure). Please read the specific supplementary information relating to Legislative Decree no. 231/2001 and to the *Whistleblowing*.

3. WILL YOU ALSO PROCESS MY SENSITIVE PERSONAL DATA?

Yes, we will process your sensitive personal data in order to fulfil our or your obligations and exercise your rights in the field of labour law and social security and social protection, insofar as it is authorised by applicable law or by a collective agreement (*art. 9, sec. 2, let. b) of the Regulation*). The processing may concern:

a) in the context of data disclosing religious, philosophical or other beliefs, or membership of associations or organisations of a religious or philosophical nature, data concerning the use of religious leave and holidays or canteen services, as well as the expression, in the cases provided for by law, of conscientious objection;
b) in the context of data disclosing political opinions, membership of political parties, trade unions, associations or organisations of a political or trade union nature, data concerning the exercise of public functions and political offices, trade union activities or offices (provided that the processing is carried out for the purpose of taking leave of absence or leave of absence recognised by law or, where applicable, by collective agreements, including company agreements), or the organisation of public initiatives, as well as data relating to deductions for the payment of membership fees for trade unions, political or trade associations or organisations;
c) in the context of data disclosing health, data collected and further processed in relation to disability, infirmity, pregnancy, childbirth or breastfeeding, accidents, exposure to risk factors, psycho-physical suitability to carry out certain tasks, membership of certain protected categories, as well as data contained in the health certificate attesting to the state of illness, including occupational illness of the person concerned, or in any case relating to illness as a specific cause of absence of the worker.

4. IS IT COMPULSORY OR OPTIONAL TO PROVIDE DATA?

The provision of personal data is optional but necessary, as failure to do so will make it impossible to enter into an employment contract with us and to fulfil it. If the data are requested on each occasion in order to take part in company initiatives in which it is possible to participate on an optional basis or in order to obtain possible benefits from the company at the request of the person concerned (for example, in the case of the concession of a company car), the provision of the relative data is optional and if it is not provided, the only consequence will be the impossibility of taking part in the initiative or obtaining the possible benefits requested by the person concerned.

5. HOW WILL MY PERSONAL DATA BE PROCESSED AND FOR HOW LONG WILL IT BE STORED?

Your personal data will be processed with automated and non-automated tools. Specific security measures are taken to prevent data loss, unlawful or incorrect use and unauthorised access. Your personal data relating to the employment relationship (contractual data; data relating to salaries, deductions and social security contributions; etc.) will be kept for 10 years from the date on which the employment contract concluded between us ceases to be effective or from the date of any act interrupting the statutory limitation period. In addition, in order to ascertain whether any unlawful acts and/or behaviour damaging to the company's image or assets have been committed, the content of correspondence carried out via email and the other technological resources entrusted to you shall be stored, after deletion of the relevant email account (to be carried out upon termination of the employment relationship) and subsequent duplication of said content on separate and protected company servers, for a period of 10 years from the termination of the employment relationship between us.

6. WHO COULD HAVE ACCESS TO MY PERSONAL DATA?

Your personal data may be disclosed to our employees and collaborators who deal with personnel management. In addition, the following categories of subjects may become aware of your personal data, who, as data processors, provide us with services instrumental to the performance of our activities: suppliers of IT services; suppliers of management services; suppliers of administrative services; professionals and consultants; companies in our corporate group that provide us with intra-group services; external auditing companies, where present; accountants; payroll processing companies; company doctors.

7. WILL MY PERSONAL DATA BE DISCLOSED TO THIRD PARTIES?

Your data may be communicated to third parties belonging to the following categories: public bodies responsible for labour and social security matters (INAIL; INPS; etc.); the financial administration, in the cases required by law; banks and payment institutions, to the extent necessary to make or receive payments in connection with the employment relationship; social security and supplementary health care funds, including company funds; trade union associations (in the event of registration of the person concerned); trade union representatives, in fulfilment of specific obligations deriving from CCNL, CIA and company agreements; insurance companies, in order to pursue our legitimate interest in

covering our risks related to the execution of the employment relationship; travel agencies and transport companies, to allow you to make business trips; judicial authorities or police forces, in case we have to report a crime or, in any case, where necessary to pursue our legitimate interest in exercising or defending a right in court; lawyers and law firms, where necessary to pursue our legitimate interest in exercising or defending a right in court and out of court; long-term car rental companies third-party companies that have acquired our company or a branch of our company or have carried out other corporate transactions with us.

Your name, surname, company position and company contact details may be communicated to the various parties with whom the company has business relations from time to time (customers; suppliers; consultants; etc.), to the extent that this is strictly necessary for the performance of your work for the company.

We would also like to inform you that the company has a so-called intranet, on which your name, surname, company position and company contact details are published. If we decide to publish a photograph of you on our intranet, we will only do so after asking for and obtaining your optional consent. If you do not consent, you will not suffer any detrimental consequences.

Unless you have given us consent to publish your personal data (*art. 6., sec. 1, let. a) of the Regulation*) or granted a release to use your image (*art. 6, sec.1, let. b) of the Regulation*), in no other case will your data be subject to dissemination.

8. WILL MY PERSONAL DATA BE TRANSFERRED OUTSIDE THE EUROPEAN ECONOMIC AREA?

Your data may be transferred outside the territory of the European Economic Area to third parties who provide services instrumental to the creation and management of the platform through which you can make reports pursuant to Law 179/2017 (Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship-whistleblowing).

In any case, as regards transfers outside the European Economic Area, your data will be processed in compliance with current national and EU legislation, with particular reference to articles 45 et seq. of Regulation (EU) 2016/679, as well as with the requirements of the Italian Data Protection Authority. The transfer will take place after signing the typical clauses, provided by the Guarantor, which ensure an adequate level of protection of your data, even when processed by subjects outside the European Economic Area.

Please also bear in mind that when you interact for work purposes, including through the exchange of emails, with colleagues who work for companies in our group, customers, suppliers, consultants and other subjects who are based or located in countries that do not belong to the European Economic Area, some of your personal data (name, surname, job position, company contacts) will be transferred to such third countries in compliance with the guarantees referred to in the previous paragraph.

9. WHAT ARE MY RIGHTS?

You have the right to exercise at any time, free of charge and without formality, the following rights under articles 15 to 22 of the Regulation: the right to request access to your personal data (i.e. the right to obtain confirmation from us as to whether or not data concerning you is being processed and, if so, to obtain access to your personal data, receive a copy of it, and the information referred to in art. 15 of the Regulation); to correct it (i.e. the right to have inaccurate data concerning you corrected or incomplete data supplemented) or have it deleted (i.e. the right to have data concerning you deleted, if one of the reasons indicated in art. 17 of the Regulation apply); to limit its processing (i.e. the right to have your data marked in the cases indicated in art. 18 of the Regulation, in order to limit its processing in the future), as well as the right to data portability (i.e. the right, in the cases indicated in art. 20 of the Regulation, to receive from us, in a structured format, in common use and readable by automatic device, the data concerning you, as well as to transmit such data to another Data Controller without hindrance). You also have the right to revoke your consent at any time. The revocation of consent will not affect the lawfulness of processing based on consent before the revocation. We remind you that you always have the possibility to lodge a complaint with the Data Protection Authority (**www.garanteprivacy.it**) or to another supervisory authority of the Member State of the European Union in which you reside or work.

10. DOES THE REGULATION ALSO GIVE ME THE RIGHT TO OBJECT TO THE PROCESSING?

Yes, you have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you pursuant to art. 6(1)(e) or (f) of the Regulation, including profiling on the basis of these provisions. If your personal data is processed for direct marketing purposes, you have the right to object at any time to its processing for these purposes, including profiling to the extent that it is related to direct marketing.

11. HOW CAN I CONTACT YOU AND EXERCISE MY RIGHTS?

Requests to exercise your rights, as indicated above, may be made by email to the following address **dpo@lottomatica.com**

12. HOW CAN I CONTACT YOUR DATA PROTECTION OFFICER?

Requests can be submitted to the Data Protection Officer by email to the following address **dpo@lottomatica.com**

***

I have read the Privacy Policy and hereby give my consent to the processing of my images for the publication of my photo on my ID card and on the company intranet, as well as for the processing of my images in connection with any audio/video recordings that may be carried out during participation in events and/or training courses/webinars organised by the Data Controller and specified in point 1 d) of the information notice, aware that such images may be used both for internal use and for dissemination to third parties, within the limits, for the purposes and for the duration specified in the information notice, as detailed above.

☐ I GIVE MY CONSENT

☐ I DO NOT GIVE MY CONSENT

SIGNATURE

ROME, _____ _____

10. INFORMATION TO CANDIDATES

PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 (GENERAL REGULATION ON DATA PROTECTION)

We wish to inform you that Regulation (EU) 2016/679 (hereinafter, the "**Regulation**") and the relevant Italian implementing legislation establish rules on the protection of natural persons in the framework of personal data processing and safeguard the fundamental rights and freedoms of natural persons, and in particular the right to the protection of personal data. In accordance with arts. 13 and 14 of the Regulation, hereinafter we inform you of the modalities and purposes by/for which Lottomatica S.p.A. and the other companies of the Lottomatica Group (i.e., Lottomatica S.p.A. and the other companies owned and/or controlled by it, even indirectly), each as a Controller, will process your personal data. We kindly ask you to carefully read this privacy notice before supplying to us personal data that concern you or, where requested, agreeing to their processing. Please consider that this privacy notice concerns the processing of the personal data of candidates wishing to take up positions of work with us.

***

1. HOW HAVE MY PERSONAL DATA BEEN OBTAINED?

We collect your personal data directly from you when you spontaneously send us a Curriculum Vitae, when you fill out the "Work with us" form on our websites, when you answer a job advertisement or when you have a work interview with us. In some cases, we could obtain your personal data (personal details; contact data; data relating to professional training and experience; sensitive data, where applicable, on your state of health, if you belong to a protected category; other data usually contained in Curricula Vitae) from personnel selection firms, to which you have given your consent to share your personal data with us. Finally, we could obtain some of your personal data from public lists or registers and professional rolls, where, for instance, we need to verify the professional skills and qualifications you have disclosed. To this end, should you agree to give the Controller references of other persons, such persons could be contacted.

2. FOR WHICH PURPOSES WILL MY PERSONAL DATA BE PROCESSED?

We will process your personal data for the following processing purposes:

a) **In order to pursue our legitimate interests in selecting our workers** (*art. 6, par. 1, letter f), of the Regulation*)
We will process your personal data in order to pursue our legitimate interests in selecting and hiring workers who have a professional profile that meets our requirements and is consistent with the work position to which the application refers.

b) **In order to pursue our legitimate interest in assessing the working aptitude and reliability of the candidate for the exercise of specific duties** *(art. 6, par. 1, letter. f) of the Regulation)*
Also because of the public function performed by State concessionaires as well as their role in preventing the use of the financial system for the purpose of laundering the proceeds of criminal activities and the financing of terrorism (Legislative Decree no. 231/2007), we may process your judicial data, even in the form of self-certification, for the exclusive purpose of assessing whether you meet the requirements of good repute and professionalism necessary to hold senior positions (management) or to perform duties that, falling within the scope of the collection of revenue from public gaming carried out by the Controller, require the candidate to meet the above requirements of good repute and professionalism.

c) **In order to pursue our legitimate interest in verifying the absence of conflicts of interest and possession the requirement of impartiality of the candidate** *(art. 6., co. 1, let. f) of the Regulation)*
We may process your personal data together with those of your family members or close relatives, if employed by one of the companies of the Lottomatica Group, to assess the possession of the impartiality requirement and to guarantee our legitimate interest to ensure impartiality and avoid conflicts of interest, including

potential ones, within the Group, in compliance with the policy Anti Bribery & Corruption of the Lottomatica Group.

d) In order to comply with legal obligations (*art. 6, par. 1, letter c), of the Regulation*)
If you belong to a protected category, we will process your personal data concerning your state of health in order to comply with the relevant legal obligations. Furthermore, it is only in the cases specifically contemplated by law and if necessary, in connection with the position for which you are applying, that we will process your personal data, including judicial data, in order to verify subjective requisites and preconditions for disqualification.

3. IS THE SUPPLY OF THE DATA MANDATORY OR VOLUNTARY?

Supplying the personal data is voluntary, but necessary, because if they are not supplied, it will not be possible to apply for a work position with us.

In no event will the supply of the data constitute a commitment for the Controller to contact you or formulate employment or collaboration proposals.

4. HOW WILL MY PERSONAL DATA BE PROCESSED AND FOR HOW LONG WILL THEY BE PRESERVED?

Your personal data will be processed using both automated and non-automated instruments. Specific security measures are followed in order to avert the loss of data, unlawful or incorrect uses and unauthorised accesses.

Your data shall be kept in the Lottomatica Group's archives for a maximum period of 1 (one) year.

In particular, should you reply to a job advertisement regarding a specific job position open within our Group, your data shall be kept until the outcome of the evaluation of your application for such specific position, as well as (i) for the time necessary to formalize the employment relationship with one of the companies of our Group, in the event of a positive outcome of your application, or (ii) in the event of failure to formalise the employment relationship with one of the companies of our Group, for a further period of 1 (one) year from the transmission of your CV in order to assess your profile for other future employment positions in line with your characteristics.

It is understood that, in the event of a positive outcome of your application and consequent establishment of an employment relationship with one of the companies in the Lottomatica Group, your personal data shall be retained for the entire duration of the employment relationship and for a further period of 10 (ten) years after termination of the employment relationship, as better regulated in the information notice for employees and collaborators provided during the formalization of the employment relationship with one of the companies in our Group.

5. WHICH PERSONS MAY ACQUIRE KNOWLEDGE OF MY PERSONAL DATA?

Our employees and collaborators engaged in selecting personnel may acquire knowledge of your personal data. Furthermore, the following categories of persons who – in their capacity as processors - provide us with services instrumental to carrying out our business, may acquire knowledge of your personal data: suppliers of administrative services; external professionals and advisors; and Lottomatica Group companies providing intragroup services.

6. WILL MY PERSONAL DATA BE DIVULGED TO THIRD PARTIES?

No, your personal data will not be divulged to third parties.

7. WILL MY PERSONAL DATA BE TRANSFERRED OUTSIDE THE EUROPEAN ECONOMIC AREA?

No, your personal data will be processed only within the European Economic Area.

8. WHAT ARE MY RIGHTS?

You are entitled to exercise-at any time, free of charge and without any formalities–the following rights set out in arts. 15 to 22 of the Regulation: the right to ask to access the personal data (i.e., the right to receive from us confirmation as to whether or not a processing of data concerning you is in progress and, in this case, to gain access to the personal data-obtaining copies thereof–and to the information indicated in art. 15 of the Regulation) and to ask for the rectification (i.e., the right to obtain rectification of inaccurate data concerning you or the completion of incomplete data) or erasure thereof (i.e., the right to obtain the erasure of data concerning you, if one of the reasons set out in art. 17 of the Regulation exists) or the restriction of processing concerning you (i.e., the right to obtain, in the cases indicated in art. 18 of the Regulation, the marking of the preserved data, with a view to restricting their processing in future), as well as the right to portability of the data (i.e., the right, in the cases set out in art. 20 of the Regulation, to receive from us, in a structured, commonly used and machine-readable format, the data concerning you, and also to transmit such data to another controller without hindrance). Furthermore, you are entitled to withdraw your consent at any time. The withdrawal of consent does not compromise the lawfulness of processing based on the consent given prior to the withdrawal. We remind you that you can always lodge a complaint either with the personal data protection Regulator (**www.garanteprivacy.it**) or with the different supervisory Authority of the European Union Member State where you live or work.

9. DOES THE REGULATION ALSO ACKNOWLEDGE MY RIGHT TO OPPOSE THE PROCESSING?

Yes. You are entitled to oppose at any time–for reasons inherent in your particular situation–the processing of personal data concerning you, within the meaning of article 6, paragraph 1, letters e) or f) of the Regulation, including profiling, in accordance with these provisions. In cases where the personal data are processed for direct marketing purposes, you are entitled to oppose at any time the processing of personal data concerning you that is carried out for such purposes, including profiling, in so far as this is inherent in such direct marketing.

10. HOW CAN I CONTACT YOU AND EXERCISE MY RIGHTS?

Requests to exercise your rights, as indicated above, may be submitted by email to the address **dpo@lottomatica.com.**

11. HOW CAN I CONTACT YOUR DATA PROTECTION OFFICER?

Requests may be submitted by email to the address **dpo@lottomatica.com.**

11. INFORMATION WHISTLEBLOWING

PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 (GENERAL REGULATION ON DATA PROTECTION)

On December 29, 2017, the Law no. 179 establishing "*Provisions on the whistle-blower's protection for reports concerning crimes or irregularities, which the person has been aware during a public or private employment*" entered into force, in order to encourage the employees and consultants to make reports, to ensure the entity's integrity, with details of circumstances concerning unlawful conducts, which are relevant pursuant to Legislative Decree no. 231/2001, or breaches of the entity's organization and management model, which the subjects have been aware during the performance of their activities.

Lottomatica Group adopted an Organisational, Management and Control Model pursuant to Legislative Decree no. 231/2001 (hereinafter, the "**231 Model**") in order to prevent the perpetration of crimes provided for under such decree, as well as a company's procedure pursuant to Law no. 179/2017 to encourage the employees, directors, members of Company's bodies and third parties which have business relations of whatsoever kind with Lottomatica Group to report any potential breach of Code of Ethics, of the Organisational, Management and Control Model pursuant to Legislative Decree no. 231/2001, of Anti-bribery & corruption Policy and Guidelines, to the relevant law applicable to the Group as well as the internal procedure and guide-lines (so called whistleblowing).

We wish to inform you that Regulation (EU) 2016/679 (hereinafter, the "**Regulation**") and the relevant Italian implementing legislation establish rules on the protection of natural persons in the framework of personal data processing and safeguard the fundamental rights and freedoms of natural persons, and in particular the right to the protection of personal data. In accordance with arts. 13 and 14 of the Regulation, hereinafter we inform you of the modalities and purposes by/for which Lottomatica S.p.A. will process your personal data, in its capacity as controller. We kindly ask you to carefully read this privacy notice before supplying to us personal data that concern you or, where requested, agreeing to their processing. Please consider that this privacy notice concerns the processing of the personal data of the whistle-blower, if they will choose to be identified in the reporting phase, and of the reported person.

***

1. HOW HAVE BEEN MY PERSONAL DATA SUPPLIED?

In order to apply and comply with Law no. 179/2017, the Company has established a specific procedure available on the company's intranet and on the website **Whistleblowing | Lottomatica (lottomaticagroup.com)**.

By typing the following URL **EthicsPoint – Lottomatica**, the whistle-blower can fill a form to make a report and can choose, in such phase, to supply (or not) his identification data. In order to make a report, the whistle-blower has to necessarily provide the identification data and contact details of the reported person.

2. WHAT ARE THE PURPOSES OF PROCESSING MY PERSONAL DATA?

We will process your personal data for the following purposes:

a) **To comply with legal undertakings** (*art. 6, paragraph 1, let. c) of the Regulation*)
We will process your personal data to comply or to obtain the compliance with specific undertakings or to perform specific tasks provided for under the relevant European Union rules, law, regulation or collective bargaining agreements also of the company, in particular in order to apply the relevant law concerning the administrative liability of the entities and of the companies.

b) **To pursue our legitimate interests in exercising or defending a right in, or outside of, court** (*art. 6., paragraph 1, let. f) of the Regulation*)
We will process your personal data to pursue our legitimate interests in exercising or defending a right in,

or outside of, court, as well as by administrative means or through arbitration and mediation procedures in the events provided for under the relevant laws, rules both of Italy and of European Union, regulations and collective bargaining agreements, also when a breach of company's procedure or of the Model occurs.

3. WILL BE MY PERSONAL JUDICIAL DATA PROCESSED?

Yes, the employees who is in an apical or managerial position in the companies of the Lottomatica Group and the Independent Supervisory Body ("*Organismo di Vigilanza*"), a body with independent initiative and control power, which has to supervise the functioning of, effectiveness of and compliance with the 231 Model, can process the employees' personal data, in compliance with the relevant legal undertakings (art. 6, paragraph 1, let. c) of the Regulation), as well as the judicial data (or the ones related to criminal proceedings and sentences) to the extent that it will be necessary to comply with a legal duty providing adequate safeguard of rights and freedoms of the concerned person (art. 10 of the Regulation).

4. IS THE DATA-SUPPLY MANDATORY OR OPTIONAL?

The data-supply is optional for the whistle-blower, instead, in relation to the reported person, his personal data-supply is mandatory, because – in case of reports without details of circumstances – the same report shall not be taken over.

5. HOW WILL BE MY PERSONAL DATA PROCESSED AND FOR HOW LONG WILL BE THEY KEPT?

Your personal data will be processed using both automated and non-automated instruments. Specific security measures are taken to avoid the loss of data, unlawful or improper uses and unauthorized accesses. Your personal data will be kept for 5 (five) years from the receipt of the report, without prejudice of specific judicial needs to protect the rights of the controller or the companies of "Lottomatica Group".

The reports will be confidential and will be managed in order to ensure the confidentiality of the identity of the whistle-blower and of the reported person. The Company undertakes to protect the whistle-blower from any reprisals or discriminations, direct or indirect, for reasons related to, directly or indirectly, the report.

6. WHO MAY ACQUIRE KNOWLEDGE OF MY PERSONAL DATA?

Personal data of who blew the whistle or who was indicated in the report (i.e. the identification personal data of the whistle-blower/reported person – in case they are known – and the ones related to the content of the report, including eventual judicial data on criminal proceeding and sentences) will be processed in compliance with art. 6, paragraph 1, let. c) and art. 10 of the Regulation and will be brought to the knowledge of the heads of the relevant departments of the Group "Lottomatica", in order to assess the report's validity.

Whenever, following preliminary verifications, it results that the report is relevant for 231 field, the data will be transmitted to the Independent Supervisory Board ("*Organismo di Vigilanza*"). During the performance of its own activities, the Independent Supervisory Board could process the employees' personal data, in compliance with the relevant legal undertakings (art. 6, paragraph 1, let. c) of the Regulation), as well as judicial data (or the ones related to criminal proceedings and sentences) to the extent that it will be necessary to comply with a legal undertakings providing adequate safeguard of rights and freedoms of the concerned people (art. 10 of the Regulation).

The employee's personal data, including judicial ones, could be processed also by people who is in apical and managerial positions in the companies of the Group "Lottomatica" in connection with eventual breaches of the employee carried out during his working activity, in order to take the advisable measures and to allow the company and the other companies of the Lottomatica Group to pursue its legitimate interests in exercising or defending a right in court (art. 6, paragraph. 1, let. c) of the Regulation).

7. WILL BE MY PERSONAL DATA DIVULGED TO THIRD PARTIES?

Such personal data and documentation supporting the report could be divulgated to suppliers of administrative and IT services, to lawyers, law firms and other consultants which assist the company, as well as they could be transmitted to

the judicial Authority if the company considers advisable to denounce the possible breach, also to pursue its legitimate interests in exercising or defending a right in court (art. 6, paragraph. 1, let. f) of the Regulation).

8. WILL BE MY PERSONAL DATA TRANSFERRED OUTSIDE THE TERRITORY OF THE EUROPEAN ECONOMIC AREA?

Yes, your personal data may be transferred outside the territory of the European Economic Area, to suppliers of IT services related to the management of the form, through which make reports.

Anyway, your personal data will be processed and transferred in compliance with current legislation, both national and European, in according to the Regulation (EU) 2016/679, as well as in compliance with the requirements of the Authority for the Protection of Personal Data by singing model clauses, provided by the Guarantor, which ensure an appropriate level of protection of your data, even if processed by subjects outside the European Economic Area.

9. WHAT ARE MY RIGHTS?

You are entitled to exercise-at any time, free of charge and without any formalities–the following rights set out in arts. 15 to 22 of the Regulation, pursuant to and within the limits provided for by applicable law from time to time: the right to ask to access the personal data (i.e., the right to receive from us confirmation as to whether or not a processing of data concerning you is in progress and, in this case, to gain access to the personal data-obtaining copies thereof–and to the information indicated in art. 15 of the Regulation) and to ask for the rectification (i.e., the right to obtain rectification of inaccurate data concerning you or the completion of incomplete data) or erasure thereof (i.e., the right to obtain the erasure of data concerning you, if one of the reasons set out in art. 17 of the Regulation exists) or the restriction of processing concerning you (i.e., the right to obtain, in the cases indicated in art. 18 of the Regulation, the marking of the preserved data, with a view to restricting their processing in future), as well as the right to portability of the data (i.e., the right, in the cases set out in art. 20 of the Regulation, to receive from us, in a structured, commonly used and machine-readable format, the data concerning you, and also to transmit such data to another controller without hindrance). Furthermore, you are entitled to withdraw your consent at any time. The withdrawal of consent does not compromise the lawfulness of processing based on the consent given prior to the withdrawal. We remind you that you can always lodge a complaint either with the personal data protection Regulator (**www.garanteprivacy.it**) or with the different supervisory Authority of the European Union Member State where you live or work.

Please consider that, in order to protect the identity of the whistle-blower, the employee or the different person involved in the report is not entitled to exercise his rights pursuant to the Regulation, when such rights' exercise can allow to identify the whistle-blower.

10. DOES THE REGULATION ALSO ACKNOWLEDGE MY RIGHT TO OPPOSE THE PROCESSING?

Yes. You are entitled to oppose at any time–for reasons inherent in your particular situation–the processing of personal data concerning you, within the meaning of article 6, paragraph 1, letters e) or f) of the Regulation, including profiling, in accordance with these provisions. In cases where the personal data are processed for direct marketing purposes, you are entitled to oppose at any time the processing of personal data concerning you that is carried out for such purposes, including profiling, in so far as this is inherent in such direct marketing.

11. HOW CAN I CONTACT YOU AND EXERCISE MY RIGHTS?

Requests to exercise your rights, as indicated above, may be submitted by email to the address **dpo@lottomatica.com**

12. HOW CAN I CONTACT YOUR DATA PROTECTION OFFICER (DPO)?

The DPO can be submitted by email to the address **dpo@lottomatica.com**

LOTTOMATICA

www.lottomaticagroup.com