Intesi Group Spa

Via Torino 48
20123 Milano (MI)
Tel: 026760641
P.IVA 02780480964
PEC: intesigroup@ig-trustmail.com

LIST OF ADOPTED SECURITY MEASURES FOR PROCESSING ON BEHALF OF THIRD PARTIES

The Implemented security measures in accordance with art. 32 of (EU) Reg. 2016/679 are described below.

Security measures adopted at the logical and organisational level

Drafting of a training plan for processors	A training plan for employees is envisaged, to make them aware of the risks affecting the data, of the measures available to predict harmful events, of the profiles of the regulations on the protection of personal data that are most relevant in relation to the related activities, of the resulting responsibilities and how to remain up to date on the measures taken. Training is already planned at the time of entry into service, but also when changes to duties arise, or upon the introduction of new significant tools, relevant to the processing of personal data.
Periodic verification of the scope of the processing and of the authorisation profiles.	The scopes of processing authorised for processors and managers responsible for the management or maintenance of electronic systems are updated periodically, at least.
Back-up verification.	A periodic verification plan has been prepared for the correct functioning of the Back-Up copies.
Delivery of detailed instructions to the processors.	Each processor was given detailed and complete instructions regarding the processing of personal data, according to their duties and the data processed. ► Instructions for the secrecy of the authentication system and the custody of personal devices. Instructions to ensure the secrecy of the confidential component of the credential (e.g. password) and the diligent custody of the devices in the possession and exclusive use of the operator. ► Instructions on the custody of electronic instruments during processing sessions. Instructions are given to the operators not to leave the electronic tool unattended and accessible during a processing session. ► Instructions for removable media in case of sensitive or judicial data. In the case of sensitive or judicial data, organisational and technical instructions are given for the custody and use of the removable media on which the data are stored in order to prevent unauthorised access and unauthorised processing. ► Written instructions for checking and storing paper documents. The operators received written instructions on the behaviour to be followed for the entire cycle necessary for carrying out the processing operations.
Data recovery procedure.	Appropriate measures have been adopted to guarantee the restoration of access to data in the event of damage to the same or to the electronic instruments, within certain times compatible with the rights of the data subjects and not exceeding 7 days.
The Privacy Organisational Manual has been drawn up and is updated annually.	The Privacy Organisational Manual contains the documents and organisational and operational procedures to be carried out by operators when processing personal data.

Destruction of removable media.	In the case of special or judicial data, the removable media that contain such data if not used are destroyed or rendered unusable, or can be used by unauthorised personnel only after the data contained therein is made unintelligible and technically unrecoverable in any way.
Written description of the operations performed by third parties.	When external parties are used for the practical adoption of safety measures, a written description of the intervention carried out is required, which certifies its compliance with the law.
Identification of the identification details of the natural persons in charge as system administrators of the external outsourcing company.	Identification of the identification details of the natural persons in charge as system administrators of the external outsourcing company.
Annual verification carried out by System Administrators.	The work of the system administrators is verified at least annually by the Data Controller.
Drafting of the Register of Processing operations both as Controller and if necessary as Manager	The record of processing activities is a mandatory document and contains the list of processing operations carried out, any communications thereof externally and related security measures implemented.
Drafting of the Privacy by Design and By Default document	Drafting of the Privacy Plan by Design and By Default to document the implementation of the necessary security measures for all processing pursuant to art. Art. 32 able to guarantee a low residual risk
Appointment of the DPO	Appointment of the Data Protection Officer
Data Breach Management Procedure	Drafting and Implementation of structural and organisational procedures for the management of any Data Breach
Implementation of the procedure for appointing a processing manager	Implementation of the Procedure for Appointment as Processing Manager for all external facilities that process data on behalf of the Data Controller
Implementation of the procedure for verifying processing managers	Implementation of the verification procedure so that the processing operations carried out by external parties have adequate guarantees of low residual risk
Verification of the preventive assessments pursuant to Art. 5 paragraph 1 of the GDPR.	Each Data Controller pursuant to article 5 paragraph 2 must be able to give evidence of the assessment carried out before and during the data processing. The Data Controller must be able to demonstrate the compliance of its activities including the effectiveness of the security measures pursuant to Article 32 and of Privacy by Design and by Default pursuant to Article 25 of the GDPR.

Adopted security measures for data processing

- **Application maintenance on premise**

Application maintenance on premise

Ordinary Data processed:	• Ordinary personal data if provided by the client.
Type of Data processed:	• Special category of personal data if provided by the client.
Judicial Special Data processed:	• Personal data relating to criminal convictions and offences if provided by the client.
Filing units used for the processing:	• Applicativo installato presso cliente .

Adopted measures

Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password.
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing. ► Periodic verification of the authorisation profile. Periodically, and at least annually, the authorisation profiles are verified.
Adequate criteria have been adopted including the possible appointment as Manager to ensure that the external facility where the storage unit resides has adequate countermeasures that guarantee a low residual risk.	In the case of archives managed in ISP mode, it is necessary that the filing manager implements adequate security measures in order to guarantee low residual risks on processing. See the section on the record of processing activities for further information in the case of outsourced data.

- **Digital document management and preservation**

Type of Data processed:	• Data types defined by DPA.
Filing units used for the processing:	• Backup Archivi di Conservazione (fino al 2022) ; • Deleghe Digitali eW ; • Gestione e Conservazione Digitale ; • PEC Organizer per clienti eWitness .

Adopted measures

Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data). ► Written provisions for data availability. When access to data is allowed only through the use of the confidential component of the credential, suitable and preventive written instructions are given aimed at clearly identifying the ways in which the availability of data can be ensured in the event of prolonged absence or impediment of the operator. ► Deactivation of old credentials. The identification credentials are deactivated if they have not been used for at least six months (except for those previously authorised for technical management purposes only), or as soon as the operator loses the ability to access the personal data.
Encryption of stored data.	The data saved on digital archiving systems are encrypted through protection systems in SSL, PGP, or other proprietary encryption systems.
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► An authorisation system is used. Procedures and tools are defined or used that enable access to data and the methods of processing them, according to the authorisation profile. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing. ► Periodic verification of the authorisation profile. Periodically, and at least annually, the authorisation profiles are verified.
Adequate criteria have been adopted including the possible appointment as Manager to ensure that the external facility where the storage unit resides has adequate countermeasures that guarantee a low residual risk.	In the case of archives managed in ISP mode, it is necessary that the filing manager implements adequate security measures in order to guarantee low residual risks on processing. See the section on the record of processing activities for further information in the case of outsourced data.
Verification and possible appointment of system administrators if present	Verification and possible appointment of system administrators if present
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Processing of data with encrypted protocols.	Data processing with encrypted protocols e.g. SSL or data encryption via PGP
Back-up copies.	Organisational and technical instructions are given and electronic equipment is set up which requires data to be saved at least weekly. ► Daily Back-Up.

Verification and registration of the accesses of the system administrator if appointed directly by the Company	Verification and registration of the accesses of the system administrator if appointed directly by the Company

- **Hosting for eWitness**

Type of Data processed:	• Data types defined by DPA.
Filing units used for the processing:	• Gestionale eWitness .

Adopted measures

Back-up copies.	Organisational and technical instructions are given and electronic equipment is set up which requires data to be saved at least weekly. ► Daily Back-Up.
Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data). ► Deactivation of old credentials. The identification credentials are deactivated if they have not been used for at least six months (except for those previously authorised for technical management purposes only), or as soon as the operator loses the ability to access the personal data.
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► An authorisation system is used. Procedures and tools are defined or used that enable access to data and the methods of processing them, according to the authorisation profile. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing.
Adequate criteria have been adopted including the possible appointment as Manager to ensure that the external facility where the storage unit resides has adequate countermeasures that guarantee a low residual risk.	In the case of archives managed in ISP mode, it is necessary that the filing manager implements adequate security measures in order to guarantee low residual risks on processing. See the section on the record of processing activities for further information in the case of outsourced data.

Verification and registration of the accesses of the system administrator if appointed directly by the Company	Verification and registration of the accesses of the system administrator if appointed directly by the Company
Verification and possible appointment of system administrators if present	Verification and possible appointment of system administrators if present

- **IG Sign Service**

Cloud service for document approval and signing workflow, used by Intesi Group customers as Data Controllers

Ordinary Data processed:	• name, address or other personal identification data; • Phone number.
Type of Data processed:	• Data types defined by DPA.
Filing units used for the processing:	• Mandrill ; • Data Center Equinix ; • IG Sign .

Adopted measures

Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data). ► Written provisions for data availability. When access to data is allowed only through the use of the confidential component of the credential, suitable and preventive written instructions are given aimed at clearly identifying the ways in which the availability of data can be ensured in the event of prolonged absence or impediment of the operator.
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Manual suspension of work sessions.	Manual suspension of work sessions.
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► An authorisation system is used. Procedures and tools are defined or used that enable access to data and the methods of processing them, according to the authorisation profile. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing. ► Periodic verification of the authorisation profile. Periodically, and at least annually, the authorisation profiles are verified.

Adequate criteria have been adopted including the possible appointment as Manager to ensure that the external facility where the storage unit resides has adequate countermeasures that guarantee a low residual risk.	In the case of archives managed in ISP mode, it is necessary that the filing manager implements adequate security measures in order to guarantee low residual risks on processing. See the section on the record of processing activities for further information in the case of outsourced data.
Separation of health data from other personal data on electronic systems	Health data is separated in terms of viewing and storage from other personal data. In electronic filing systems it is sufficient that on the first screen the health data are not visible. Healthcare organisations have an obligation to separate health data from other personal data
Verification and registration of the accesses of the system administrator if appointed directly by the Company	Verification and registration of the accesses of the system administrator if appointed directly by the Company
Verification and possible appointment of system administrators if present	Verification and possible appointment of system administrators if present
Back-up copies.	Organisational and technical instructions are given and electronic equipment is set up which requires data to be saved at least weekly. ► Daily Back-Up.
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.

- **Not qualified signature service**

Not qualified signature service (AES and other electronic signature)

Ordinary Data processed:	• tax code and other personal identification numbers; • name, address or other personal identification data; • economical, commercial, financial and insurance activities; • personal data such as IP address and other common data managed in strictly necessary cookies; • browsing functionality cookies; • Phone number; • Video recordings; • Photos or photocopies of identity documents.
Filing units used for the processing:	• Armadio Erogazione (Site: Sede principale azienda); • Data Center Equinix .

Adopted measures

Insurance Coverage	Taking out adequate insurance coverage for events inherent to data processing relating to the GDPR
Alarm installation	Alarm installation
Extinguishers.	Fire extinguisher installation and periodic verification thereof.

Custody in non-accessible filing cabinets or cabinets	The paper-based data are archived in such a way as to allow access only to the processors and not to be accessible to unauthorised persons.
Filing system locks supplied.	If there are special or judicial data in paper-based files, a filing system lock is used.
Controlled access filing system.	Access to the filing system is controlled by those in charge of processing or surveillance. After closing time, only those previously authorised or identified and registered can access the filing system.
Checking of documents with special or legal data by the processors.	When documents containing special or judicial data are entrusted to the data processors, they are controlled and kept by them until they are returned so that they are not accessed by people without authorisation, and are returned at the end of the allocated operations.
Back-up copies.	Organisational and technical instructions are given and electronic equipment is set up which requires data to be saved at least weekly. ► Daily Back-Up.
Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data). ► Written provisions for data availability. When access to data is allowed only through the use of the confidential component of the credential, suitable and preventive written instructions are given aimed at clearly identifying the ways in which the availability of data can be ensured in the event of prolonged absence or impediment of the operator.
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Manual suspension of work sessions.	Manual suspension of work sessions.
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► An authorisation system is used. Procedures and tools are defined or used that enable access to data and the methods of processing them, according to the authorisation profile. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing. ► Periodic verification of the authorisation profile. Periodically, and at least annually, the authorisation profiles are verified.
Verification and possible appointment of system administrators if present	Verification and possible appointment of system administrators if present

- **Processing for third parties by Solution Area**

Processing by the Solutions division of personal data whose controller is a customer.

Type of Data processed:	• Data types defined by DPA.
Filing units used for the processing:	• Dispositivo individuale (Site: Smart Working).

Adopted measures

Installation of a Firewall.	In the case of the processing of personal data with electronic tools connected with the outside, even indirectly or only occasionally, it is necessary to install a software or hardware firewall to prevent unauthorised access to them. ► Firewall software. Firewall software.
Antivirus.	Antivirus programs are installed on electronic computers that contain personal data, updated at least every six months. ► Update every month.
Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data).
Software Update.	Periodic program updates, aimed at preventing vulnerability or correcting defects, are carried out taking into account that you have installed at least the version prior to the latest one available.
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Manual suspension of work sessions.	Manual suspension of work sessions.

- **Servizio SPID come Aggregatore**

Ordinary Data processed:	• tax code and other personal identification numbers; • name, address or other personal identification data; • browsing functionality cookies; • Phone number.
Filing units used for the processing:	• Data Center Equinix .

Adopted measures

Back-up copies.	Organisational and technical instructions are given and electronic equipment is set up which requires data to be saved at least weekly. ► Daily Back-Up.
Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data). ► Written provisions for data availability. When access to data is allowed only through the use of the confidential component of the credential, suitable and preventive written instructions are given aimed at clearly identifying the ways in which the availability of data can be ensured in the event of prolonged absence or impediment of the operator.
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Manual suspension of work sessions.	Manual suspension of work sessions.
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► An authorisation system is used. Procedures and tools are defined or used that enable access to data and the methods of processing them, according to the authorisation profile. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing. ► Periodic verification of the authorisation profile. Periodically, and at least annually, the authorisation profiles are verified.
Verification and possible appointment of system administrators if present	Verification and possible appointment of system administrators if present

- **Test Factory**

Testing of software products on behalf customers

Ordinary Data processed:	• name, address or other personal identification data.
Type of Data processed:	• Data types defined by DPA.
Filing units used for the processing:	• MS Office 365 & Teams ; • Google Suite .

Adopted measures

Authentication credentials, assigned individually to each employee.	Data processing is allowed only after passing an authentication procedure uniquely associated with the employee and relating to a specific processing operation or set of processing operations. Furthermore, the identification code, when used, is never assigned to other processors, not even at different times. ► Authentication by user-id and password. ► Key word of at least 8 characters. The keywords are 8 characters or the maximum allowed by the system, they must not be traceable to the operator and are changed at least every 3 months (6 if there are only common data).
Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.
Automatic suspension of work sessions.	The system automatically suspends the work session under certain circumstances (such as after a minimum time of inactivity).
Manual suspension of work sessions.	Manual suspension of work sessions.
Processing of data with encrypted protocols.	Data processing with encrypted protocols e.g. SSL or data encryption via PGP
Different scope authorisation profiles for different operators.	In the event that the operators can access only certain types of data, or carry out only some processing operations, the authorisation profiles must be diversified for each operator. ► An authorisation system is used. Procedures and tools are defined or used that enable access to data and the methods of processing them, according to the authorisation profile. ► Authorisation profiles are specified before each processing operation. Each operator is assigned their own authorisation profile before the start of processing. ► Periodic verification of the authorisation profile. Periodically, and at least annually, the authorisation profiles are verified.
Adequate criteria have been adopted including the possible appointment as Manager to ensure that the external facility where the storage unit resides has adequate countermeasures that guarantee a low residual risk.	In the case of archives managed in ISP mode, it is necessary that the filing manager implements adequate security measures in order to guarantee low residual risks on processing. See the section on the record of processing activities for further information in the case of outsourced data.
Verification and possible appointment of system administrators if present	Verification and possible appointment of system administrators if present

- **Text messaging service as Processor**

Text messaging service as second factor authentication

Ordinary Data processed:	• Phone number; • Communication content data and traffic data.
Filing units used for the processing:	• SMS di Commify (ex Mobyt) ; • SMS e messaggistica .

Adopted measures

Encryption of transmitted data.	When transmitted from one digital system to another, the data before transmission are encrypted with protection systems such as SSL, PGP, ZIP with a password or other proprietary systems. Healthcare organisations and healthcare professionals have an obligation to transmit sensitive health data using encryption systems ► Encryption with SSL protocol.