PRIVACY POLICY

Processing activities

Intesi Group, when providing services, processes personal data as follows:

1. management of required services (including online and store online services) and relevant finance, bookkeeping, invoicing, payment and credit monitoring activities and provisioning of support and updating services;
    - Intesi Group is data controller of these processing activities because it determines the purposes and means of the processing of personal data, as described in this document;
    - legal ground for the processing is the performance of a contract and the compliance with a legal obligation (bookkeeping and fiscal);
    - data are retained for 10 years after the last invoice (for the relevant bookkeeping regulations) or the end of relevant legal actions; data may be retained for an additional year, because in the backup lifecycle;
2. management of quality and customer satisfaction;
    - Intesi Group is data controller of these processing activities because it determines the purposes and means of the processing of personal data, as described in this document;
    - legal ground for the processing are the legitimate interests pursued by the controller, i.e. quality assurance;
    - data of each survey are retained for 5 years or in the project or service documentation for 10 years (this is because these documents are linked to the invoicing); data may be retained for an additional year, because in the backup lifecycle;
3. trusted service users identification;
    - Intesi Group is data controller of these processing activities because it determines the purposes and means of the processing of personal data, as described in this document;
    - legal ground for the processing is the performance of a contract and the compliance with legal obligations (trusted service providers relevant ones);
    - data are retained for 20 years after the expiration of digital certificate identification mechanisms, according to the trusted service provider applicable regulations); data may be retained for an additional year, because in the backup lifecycle;
4. management of users' documents (e.g. for signature), according to the required services;
    - Intesi Group is data processor of these processing activities because the customer determines the purposes and means of the processing of personal data;
    - data are not retained after the service provisioning; logs are retained for 20 years, according to the trusted service provider applicable regulations); data may be retained for an additional year, because in the backup lifecycle;
5. management of assistance, contact or CV requests sent through web site;
    - Intesi Group is data controller of these processing activities because it determines the purposes and means of the processing of personal data, as described in this document;
    - legal ground for the processing is the provisioning of required services and the legitimate interests pursued by the controller, i.e. quality assurance;
    - data are retained for one year after the service provisioning in order to perform quality controls (CV sare retained for 10 years, unless different agreement with data subjects); data may be retained for an additional year, because in the backup lifecycle;
6. web site management, using cookies (see below);
    - Intesi Group is data controller of these processing activities because it determines the purposes and means of the processing of personal data, as described in this document;
    - legal ground for the processing is the legitimate interest pursued by the controller, i.e. quality assurance;
    - data are retained in cookies on the user's pc and their lifespan is set one year;
7. social network pages management and, with tools given by the social network (it can also cookies and other tracking tools), activity analysis, relations with users, sharing of non private posts and other activities available by the social network;

- Intesi Group is a joint data controller, with the social network itself (the social network has its own privacy policy);
- legal grounds for the processing are the consent of data subjects (given when registering to the social network), the need to answer to requests of users, the legitimate interest pursued by the controller (tracking of communications with users, brand evaluation, marketing);
- data are retained by the social network, according to their rules.

Privacy contact point

Intesi Group appointed a privacy focal point, with the duty to monitor the fairness of processing activities of Intesi Group itself. Privacy contact point has email address privacy@intesigroup.com.

Transfer of personal data

For the above purposes, Intesi Group may transfer personal data to external legal entities or people.

Examples are entities for bookkeeping and accountability purposes; quality and security assurance of trusted services; legal, administrative and tax consultants; couriers for the transportation of documents and assets; banks; mail services.

External providers and suppliers agreed, with written contracts, to process data only for the stated purposes and adopt suitable security measures and processing controls. The list of external providers and suppliers is available from the privacy contact point. Data controllers, where Intesi Group is data processor, always authorize the change, by Intesi Group, of these subjects.

All external subjects ensure their assistance for the fulfilment of the obligations to respond to requests for exercising the data subject's rights and audit right.

Transfers to third Countries

Data are not transferred in extra-EEA Countries.

Contact data, used for updating customers with mailing lists, are transferred abroad (USA). Mailing platforms adhere to Privacy Shield (www.privacyshield.gov) protocol, considered as a mechanism for ensuring the security, correctness and lawfulness of the processing of personal data.

Security measures

Intesi Group adopts security measures for protecting data. Among them:

- all people authorized to access and process data is aware of behaviors to enforce (e.g. for IT devices, email, passwords) and is committed to confidentiality;
- a process is established for the provisioning, change, deletion and review of access authorizations to data; the process implements *need-to-know* and *need-to-use* principles;
- measures are established in order to reduces as much as possible the authorizations of privileged users of IT systems (i.e. systems administrators) and to log their activities (e.g. giving them only personal user-ids and activating log systems);
- a process is established for the deletion of data and memory devices so that unauthorized persons cannot retrieve data anymore;
- physical security controls are enforced for blocking access to information on hardcopy support to unauthorized persons;
- IT security measures are implemented according to the level of risk (e.g. activation and regular update of antimalware systems, data backups, activity logging and log retention, regular patching and fixing, network and Internet traffic filtering, portable device encryption);
- a process is established for the change management (for IT base systems, network and applications, processes, physical security controls); this process include the evaluation of the effectiveness of security measures;

- suppliers ensure in contracts they enforce information security according to the given level of risk and instructions;
- a process is established for the incident (data breach) management that includes prevention and impact control and, in some cases, communication to the Data protection authority and data subjects;
- a process is established for the evaluation of the effective implementation of security measures; this process includes audits to relevant data processors.

Additional measures for trusted services are described in documents available on our web site (https://www.intesigroup.com/it/documenti).

Intesi Group has a quality and information security management systems certified under the accreditation scheme controlled by the European regulations.

Additional measures

Intesi Group ensures its support to the customer if necessary:

- for the fulfilment of the obligations to respond to requests for exercising the data subject's rights and audit right;
- in case of personal data breach and information security incidents;
- for carrying on privacy risk assessment and privacy impact assessment;
- for deleting or destroying personal data at the end of the contractual obligations;
- for answering to the relevant data protection authorities.

Intesi Group gives to its customers the right of audit, provided that audits will only analyse relevant processing activities, confidentiality is ensured and they are announced at least 30 days earlier.

Data subject rights

Data subjects have specific rights. Among them:

- the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data, their rectification and erasure, the restriction of their processing, data portability (i.e. receiving them in a structure accessible with the most common tool); requests will not have any impacts on the provided services;
- the right to revoke the consent, if not against applicable laws or regulations;
- the right to send a complaint to Intesi Group or the Data protection authority (in Italy it is the Garante per la protezione dei dati personali).

Requests and complaints can be sent to privacy@intesigroup.com.

Cookies privacy notice

Cookies are files archived on your browser and set by the visited websites. This site only uses “technical cookies”, needed to improve the quality of the look & feel of our pages. This does not require the consent of the visitors. Intesi Group installs other cookies (by Intesi Group itself or by other entities), needed to have stastical and anonymous data about the use of the pages of the website. They are “analytics cookies” and they don’t need your consent for working:

- Google Analytics (https://support.google.com/analytics/answer/2763052?hl=it).

All users can stop the use of all or some cookies following some configuration steps for the browser:

- Chrome (https://support.google.com/accounts/answer/61416?hl=en);
- Firefox Mozilla (https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences);
- Internet explorer e MS Edge (https://support.microsoft.com/en-gb/help/278835/how-to-delete-cookie-files-in-internet-explorer);
- Opera (http://help.opera.com/Windows/10.00/en/cookies.html).

Information specific for mobile apps

Our mobile apps have the same purposes described above:

- management of required services;
- identification of users of services;
- processing of documents of users.

Apps require some authorizations for properly working. They include:

Authorization	**Reason**
Write External Storage Read Externalstorage	When a signature is approved, the document can (locally or on an external devices) be downloaded so it can be viewed. In other cases, the user can required to process some documents (for upload, download, encryption, signature) and this requires the use of the storage.
Read Phone State	Some apps use an API that needs this authorization for creating an identification code of the device.
Camera	Some apps require the use of the camera for scanning QR Codes on user's request. If the app is used for the identification of the user, then the app can need to record a video or to shot photos.
Microphone	If the app is used for the identification of the user, then the app can need to record a video (with audio).
Gallery	If the app is used for the identification of the user, then the app can need to shot photos and then to have them sent.
Location	This is needed by anti-bribery tools.
GetAcounts Read Contacts	This is used only by apps linked to other services (Dropbox, Google Drive etc...) and if the user requires to manage all their accounts.

8 June 2018