

Appendice al Supplemento per il Trattamento dei Dati Personali

Nella presente Appendice al Supplemento per il Trattamento dei Dati Personali (nel seguito per brevità "Appendice DPA") si precisa il trattamento dei dati personali per il Servizio che Intesa le fornisce.

1. Trattamento dei Dati Personali

Intesa tratterà i Dati Personali del Cliente nell'ambito del Servizio, come descritto nel contratto di riferimento e come integrato e precisato nella presente Appendice DPA.

1.1 Attività di Trattamento dei Dati Personali

Il trattamento dei Dati Personali del Cliente consisterà nelle seguenti operazioni:

- La Copia
- La Cancellazione
- La Lettura
- La Ricezione
- L'Invio
- La Memorizzazione
- L'Aggiornamento

2. Dati Personali del Cliente

2.1 Categorie di Interessati

L'elenco che segue contiene informazioni sulle Categorie di Interessati i cui Dati Personali possono essere trattati nell'ambito del Servizio:

- I dipendenti del Cliente (inclusi i lavoratori a tempo determinato o occasionali, i volontari, lavoratori in distacco, i tirocinanti, i pensionati, le pre-assunzioni e i candidati)
- I dipendenti delle consociate del Cliente (inclusi i lavoratori a tempo determinato o occasionali, i volontari, lavoratori in distacco, i tirocinanti, i pensionati, le pre-assunzioni e i candidati)
- I clienti (potenziali) del Cliente (se tali clienti (potenziali) sono persone fisiche)
- I dipendenti (potenziali) dei clienti del Cliente
- I business partner del Cliente (se tali business partner sono persone fisiche)
- I dipendenti dei business partner del Cliente
- I visitatori del Cliente

- I fornitori e subappaltatori del Cliente (se tali fornitori e subappaltatori sono persone fisiche)
- I dipendenti dei fornitori e dei subappaltatori del Cliente
- Gli agenti, consulenti e altri esperti professionisti del Cliente (fornitori)

Data la natura dei Servizi, il Cliente riconosce che Intesa non è in grado di verificare o gestire il suddetto elenco di Categorie di Interessati. Pertanto, il Cliente comunicherà a Intesa qualsiasi modifica necessaria del suddetto elenco per iscritto. Intesa tratterà i Dati Personali di tutti gli Interessati sopra elencati in conformità a quanto previsto nel Contratto. Se le modifiche dell'elenco di Categorie di Interessati richiedono modifiche rispetto al Trattamento concordato, il Cliente dovrà fornire Istruzioni Aggiuntive a Intesa come stabilito nel DPA.

2.2 Tipologie e Categorie Speciali di Dati Personali

2.2.1 Tipologie di Dati Personali

Il seguente elenco indica quali Tipologie di Dati Personali del Cliente possono essere trattate nell'ambito del Servizio:

- **Capacità e Qualifiche del Soggetto**
 - Informazioni Professionali e Occupazionali
 - Associazioni Professionali
- **Caratteristiche del Soggetto**
 - Dati Biometrici
 - Procedimenti e Condanne Penali
 - Dati Demografici
 - Dati Economici e Finanziari
 - Cartella Clinica e Informazioni Sanitarie
 - Nazionalità e Cittadinanza
 - Opinione
 - Preferenze e Interessi Personali
 - Origine Razziale o Etnica
 - Convinzioni Religiose o Filosofiche
- **Identità del Soggetto**
 - Identità Nazionali
 - Numero di Identificazione
 - Soggetto
 - Accesso Online e credenziali di Autenticazione
 - Connessione Online e dati di Connettività di Rete

- Identificativo Online
- Nome della Persona
- Identificativi Tecnologici
- Telefonia
- **Ubicazione del Soggetto**
 - Appuntamenti, Programmi e Voci di Calendario
 - Ubicazione Fisica del Soggetto

2.2.2 **Categorie Speciali di Dati Personali**

Il seguente elenco indica quali Categorie Speciali dei Dati Personali del Cliente possono essere trattate nell'ambito del Servizio:

- Dati Personali che rivelano l'origine razziale o etnica
- Dati Personali che rivelano le opinioni politiche
- Dati Personali che rivelano le convinzioni religiose o filosofiche
- Dati Personali che rivelano l'appartenenza sindacale
- Dati biometrici
- Dati riguardanti la salute
- Dati Personali relativi a reati e condanne penali

2.2.3 **Disposizioni Generali**

Gli elenchi indicati negli articoli 2.2.1 e 2.2.2 contengono informazioni sulle Tipologie e Categorie Speciali di Dati Personali del Cliente possono essere trattate nell'ambito del Servizio.

Data la natura dei Servizi, il Cliente riconosce che Intesa non è in grado di verificare o gestire i suddetti elenchi di Tipologie di Dati Personali del Cliente e Categorie Speciali di Dati Personali del Cliente. Pertanto, il Cliente comunicherà a Intesa qualsiasi modifica necessaria dei suddetti elenchi per iscritto, entro 30 (giorni) dall'intervenuta necessità di modifica. Intesa tratterà le Tipologie e le Categorie Speciali di Dati Personali del Cliente elencati sopra in conformità con il di contratto di riferimento tra Intesa e il Cliente. Se le modifiche degli elenchi di Tipologie e Categorie Speciali di Dati Personali del Cliente richiedono modifiche al Trattamento concordato, il Cliente dovrà fornire Istruzioni Aggiuntive a Intesa come stabilito nel DPA.

3. **Misure Tecniche e Organizzative**

È possibile trovare le misure tecniche e organizzative (technical and organizational measure, TOM), applicabili al servizio, in allegato alla presente Appendice DPA come Appendice 1. Il Cliente si impegna a implementare le TOM appropriate nell'ambito della propria area di responsabilità come richiesto dalle Leggi sulla Protezione dei Dati in vigore.

4. Cancellazione e Restituzione dei Dati Personali del Cliente

Intesa cancellerà i dati del Cliente al termine del Servizio, salvo diversamente stabilito nel contratto di riferimento. Tuttavia, se il Cliente desidera ottenere una copia dei Dati Personali di cui è Titolare ed il contratto di riferimento non prevede questa opzione, il Cliente stesso potrà richiedere tale copia ad Intesa prima del termine del contratto di riferimento. In tal caso, Intesa consegnerà al Cliente una copia dei suoi Dati Personali cui Intesa ha accesso in un ragionevole periodo di tempo e in un formato ragionevole a spese del Cliente stesso, in accordo con le condizioni contenute nel DPA con riferimento all'Assistenza.

5. Subresponsabili

Intesa può utilizzare i Subresponsabili elencati nelle tabelle che seguono per il Trattamento dei Dati Personali del Cliente.

Il Cliente può identificare i Subresponsabili coinvolti nei servizi acquistati dalle descrizioni dei vari servizi sotto riportate. La seguente lista di subprocessor è confidenziale.

- **Trusted Hub**

(Software and EDI Services, and all services from EDI portals or services for the exchange of documents in structured format, the special community are included, eg. Euritmo.)

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT

DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
FASTWEB SPA	VIA CARACCIOLO, 51 MILANO (MI) 20155, IT
LANTECH SOLUTIONS S.P.A.	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
O.& S.I. SRL	Via Goldoni, 27 CERRO MAGGIORE (MI) 20023 IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
SKEBBY - MOBILE SOLUTION S.r.l.	VIA MELZO 12 MILANO (MI) 20129, IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT
TECHEDGE SpA	VIA CALDERA, 21 MILANO (MI) 20153, IT

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

- **Trusted Payments**

(Treasury HUB, CBK, and all Services for the exchange of banking documents between companies or between companies and banks.)

a.

IBM companies located in the European Economic Area or countries considered by	
---------------------------------------------------------------------------------------	--

the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
FASTWEB SPA	VIA CARACCILOLO, 51 MILANO (MI) 20155, IT
LANTECH SOLUTIONS S.P.A.	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT
TAS SpA	Via Del Lavoro, 47 CASALECCHIO DI RENO (BO) 40033, IT
ICCREA BANCA SpA Ist.Centrale Credito Cooperativo	VIA LUCREZIA ROMANA, 41/47 ROMA (RM) 00178, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have	
-----------------------------------------------------------------------------------------------------------------------------------------------------------	--

adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

▪ **Trusted Logistics**

(Delivery Control and On Demand Logistics)

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO

	BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
FASTWEB SPA	VIA CARACCIOLO, 51 MILANO (MI) 20155, IT
LANTECH SOLUTIONS S.P.A.	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT
M B M ITALIA SRL	VIA L. PELLIZZO, 14/A PADOVA (PD) 35128, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
Name of IBM Data Importer	Address of IBM Data Importer
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

- **Trusted Sign**

- PEC

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
FASTWEB SPA	VIA CARACCIOLO, 51 MILANO (MI) 20155, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
NAMIRIAL SpA	VIA CADUTI SUL LAVORO 4, SENIGALLIA (AN) 60019, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
STUDIO INFORMATICA S.r.l.	STRADONE FARNESE, 43/a, PIACENZA (PC) 29121, IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT
LANTECH SOLUTIONS S.P.A.	Via Romolo Bitti n. 6 Milano (MI) 20125, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have	
-----------------------------------------------------------------------------------------------------------------------------------------------------------	--

adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

- PKI, digital certificates, remote digital signature, on-boarding services, video identification

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT

COLT TECHNOLOGY SERVICES SpA DIMENSION DATA ITALIA S.p.A.	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
FASTWEB SPA	VIA CARACCILOLO, 51 MILANO (MI) 20155, IT
ITAGILE S.R.L	PIAZZA MARCONI 15 ROMA (RM) 00144, IT
INVENTIA S.r.l.	Via Antonio Fontanesi 4 Milano (MI) 20146, IT
INTESI GROUP SpA	VIA TORINO, 48 MILANO (MI) 20123, IT
INNOVERY SPA	VIA CRETA, 78 BRESCIA (BS) 25124, IT
LANTECH SOLUTIONS S.P.A	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
NAMIRIAL SpA	VIA CADUTI SUL LAVORO 4, SENIGALLIA (AN) 60019, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
SKEBBY - MOBILE SOLUTION S.r.l.	VIA MELZO 12 MILANO (MI) 20129, IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>

NONE	
------	--

- **Graphometric Signature**

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
DIMENSION DATA ITALIA S.p.A	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
FASTWEB SPA	VIA CARACCILOLO, 51 MILANO (MI) 20155, IT
KALYOS SRL	VIA DEI MESTIERI 15 CONCOREZZO (MB) 20863, IT
LANTECH SOLUTIONS S.P.A	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
NAMIRIAL SpA	VIA CADUTI SUL LAVORO 4, SENIGALLIA (AN) 60019, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

▪ **Trusted Doc**

(Services of legal archiving and consultation of the documents stored)

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the	
-------------------------------------------------	--

European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
ARCHIVIUM SRL	CORSO FRANZIA, 233 int. D RIVOLI (TO) 10098, IT
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
eGLUE SRL	Via degli Alpini, 34 Segrate (MI) 20090, IT
FASTWEB SPA	VIA CARACCIOLO, 51 MILANO (MI) 20155, IT
LANTECH SOLUTIONS S.P.A.	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
S.D.M.	VIA DALMAZIA 31 ROMA (RM) 00198, IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
Name of IBM Data Importer	Address of IBM Data Importer
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the	
------------------------------------------------------------------------------------	--

European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

▪ **Trusted Invoice**

(Services of e-invoicing using special portals powered by In.Te.S.A. S.p.A or by means of paper mail or electronic mail services or also via connectors to the “Sistema di Interscambio statale” (SdI) for the invoicing to the Public Administration or in the private sector.)

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
ABRAMO PRINTING & LOGISTICS SPA	LOCALITA' DIFESA, ZONA INDUSTRIALE, CARAFFA DI CATANZARO (CZ) 88050, IT
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo,

	(MI) 20068, IT
FASTWEB SPA	VIA CARACCIOLO, 51 MILANO (MI) 20155, IT
LANTECH SOLUTIONS S.P.A.	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
LEADERFORM SPA	Via Molina, 14SONA VR 37060 ITA
NEXIVE SpA	VIA GAUDENZIO FANTOLI, 6/3 MILANO MI 20138 ITA
O.& S.I. SRL	Via Goldoni, 27 CERRO MAGGIORE (MI) 20023 IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
REAL DOCUMENT SOLUTION SRL-DELIVERY TICINO ITALIA	VIA A. VILLA, 10 VILLASANTA (MB) 20852, IT
S.A.T.A. APPLICAZIONE TECNOLOGIE AVANZATE SRL	Via Notari, 103 MODENA (MO) 41126, IT
SKEBBY - MOBILE SOLUTION S.r.l.	VIA MELZO 12 MILANO (MI) 20129, IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT
TECHEDGE SpA	VIA CALDERA, 21 MILANO (MI) 20153, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

▪ **EDM/BPM**

(Documents management services and digital process management services)

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
ADIUTO NET SRL	VIA E. BERNARDI 1 RUBANO (PD) 36030, IT
AT&T GLOBAL NETWORK SERVICES ITALIA SRL	VIA LIVORNO, 60 TORINO (TO) 10144, IT
CALL & CALL HOLDING Spa	VIA MASSIMO GORKI 30/32 CINISELLO BALSAMO (MI) 20092, IT
COLT TECHNOLOGY SERVICES SpA	VIA SIMONE MARTINI, 127 ROMA (RM) 00142, IT
DIMENSION DATA ITALIA S.p.A.	Via G. Di Vittorio, 24 Peschiera Borromeo, (MI) 20068, IT
FASTWEB SPA	VIA CARACCILOLO, 51 MILANO (MI) 20155, IT
LANTECH SOLUTIONS S.P.A	Via Romolo Bitti n. 6 Milano (MI) 20125, IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
REAL DOCUMENT SOLUTION SRL-DELIVERY TICINO ITALIA	VIA A. VILLA, 10 VILLASANTA (MB) 20852, IT
TELECOM ITALIA SPA	PIAZZA DEGLI AFFARI, 2 MILANO (MI) 20123 IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

- **PEC Orchestrator, for managing and organising PEC mail boxes.**

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission	
---------------------------------------------------------------------------------------------------------------------------	--

to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
STUDIO INFORMATICA S.r.l.	STRADONE FARNESE, 43/a, PIACENZA (PC) 29121, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

▪ **Services partially or totally supplied on Cloud**

a.

IBM companies located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
IBM ITALIA SPA	CIRCONVALLAZIONE IDROSCALO, SEGRATE MILANO, 20090, IT

b.

Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection	
<u>Name of Subprocessor</u>	<u>Address of Subprocessor</u>
ADIUTO NET SRL	VIA E. BERNARDI 1 RUBANO (PD) 36030, IT
O.& S.I. SRL	Via Goldoni, 27 CERRO MAGGIORE (MI) 20023 IT
PRESENT SPA	STRADA DELLA CEBROSA 86 TORINO (TO) 10156 IT
S.A.T.A. APPLICAZIONE TECNOLOGIE AVANZATE SRL	Via Notari, 103 MODENA (MO) 41126, IT
STUDIO INFORMATICA S.r.l.	STRADONE FARNESE, 43/a, PIACENZA (PC) 29121, IT

c.

IBM Data Importers (IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of IBM Data Importer</u>	<u>Address of IBM Data Importer</u>
NONE	

d.

Third Party Data Importer (non-IBM companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)	
<u>Name of Third Party Data Importer</u>	<u>Country in which Third Party Data Importer is located</u>
NONE	

Intesa tenderà di informare il Cliente sulle modifiche relative ai Subresponsabili entro un ragionevole periodo di tempo.

6. Trasferimento internazionale di dati & Clausole Contrattuali Standard UE

Le Clausole Contrattuali Standard UE, se necessarie, saranno allegate al contratto di riferimento.

7. Responsabile della Protezione dei Dati e altri Titolari del Trattamento dei Dati

Il Cliente è responsabile di fornire informazioni complete, esatte e aggiornate riguardanti (a) i suoi Responsabili della Protezione dei Dati e (b) ogni altro Titolare del Trattamento dei Dati (inclusi quelli riguardanti i Responsabili della Protezione dei Dati alternativi o aggiuntivi). Il Cliente comunicherà per iscritto a Intesa tutte le modifiche riguardanti (a) i Responsabili della Protezione dei Dati o (b) altri Titolari del Trattamento dei Dati entro 30 giorni da qualsiasi incarico o modifica.

8. Referente Intesa per la Privacy

Il contatto sulla privacy Intesa è disponibile al seguente indirizzo email: privacy_dep@intesa.it

Allegato 1 all'Appendice al Supplemento per il Trattamento dei Dati Personali per GTS

Sezione 3: Misure Tecniche & Organizzative

Le TOM definite in questo documento si applicano al Supplemento per il Trattamento dei Dati Personali allegato al Servizio Integrated Managed Infrastructure (IMI), ed a qualsiasi applicazione, piattaforma e componenti di infrastrutture sottostanti eseguite e gestite da Intesa per fornire il Servizio (componenti), eccetto quando il Cliente è responsabile della sicurezza e della privacy e come diversamente specificato nel Documento d'Ordine.

1. Dichiarazione di Adesione ai Principi di Privacy e Sicurezza

Intesa manterrà e seguirà le politiche e le procedure di sicurezza IT che sono parte integrante delle attività di Intesa e obbligatorie per tutti i suoi dipendenti, incluso il personale aggiuntivo. Le politiche Intesa sono state create in considerazione di linee guida e standard di sicurezza riconosciuti a livello internazionale, quali ad esempio le pratiche ISO 27002+-series, ed altri principi di gestione della privacy e della sicurezza quali ad esempio "Privacy by Design". Intesa riesaminerà le sue politiche di sicurezza IT almeno una volta all'anno e modificherà tali politiche quando lo riterrà ragionevole per preservare la protezione degli ambienti dei servizi dell'infrastruttura e dei dati gestiti al suo interno.

Intesa manterrà e seguirà i propri requisiti standard di verifica relativi all'occupazione, tra cui quelli relativi all'assunzione dei propri dipendenti e del personale aggiuntivo. In conformità con i processi e le procedure interne di Intesa, questi requisiti saranno periodicamente revisionati e includeranno, a titolo esemplificativo ma non esaustivo, il controllo dei precedenti penali, la prova di convalida dell'identità e ulteriori controlli, qualora ritenuto necessario. Ciascuna società del gruppo IBM, di cui Intesa fa parte, è tenuta ad implementare questi requisiti nel relativo processo di assunzione, quando applicabile e consentito dalla normativa locale.

I dipendenti Intesa ogni anno completeranno la formazione sulla sicurezza e sulla protezione dei dati e certificheranno ogni anno di attenersi agli obblighi etici riguardanti le politiche sulla riservatezza, la sicurezza e la condotta aziendale, come stabilito nel documento Business Conduct Guidelines ("Linee Guida IBM sul Comportamento Aziendale"). Ulteriore formazione sulle politiche ed i processi interni sarà impartita alle persone cui viene fornito l'accesso amministrativo ai componenti del servizio GTS, in modo specifico per loro rispettivo ruolo all'interno delle operazioni e del supporto in relazione all'utilizzo del servizio.

Intesa implementa misure di sicurezza fisiche ed ambientali per proteggere l'infrastruttura fisica, che gestisce attraverso i servizi dell'infrastruttura o gli accordi di outsourcing, da minacce ambientali, causate sia da eventi naturali, sia umani quali, ad esempio, eccessiva temperatura dell'ambiente, incendi, inondazioni, umidità, furti e vandalismo.

Intesa dispone di politiche e procedure aggiornate per gestire le sospette violazioni della sicurezza e della privacy, e fornisce una formazione annuale sulla sicurezza informatica e sulla privacy a tutti gli impiegati, relativa alla segnalazione degli incidenti legati alla sicurezza coinvolgendo dipendenti, fornitori, clienti o asset. Tali incidenti possono includere furto, minacce, atti di violenza e di vandalismo. Intesa collaborerà a stretto contatto con i propri clienti durante le attività di indagine e di segnalazione degli incidenti di violazione della sicurezza, per supportare la comunicazione delle informazioni ai clienti finali del cliente ed ai regolatori.

Ulteriori politiche e procedure che supportano la protezione dei dati includono controlli quali: la documentazione dei controlli operativi, la presenza di un processo di gestione delle modifiche di sistema, la creazione di protocolli di resilienza e backup, l'installazione di protezioni da malware aggiornate ed altre procedure che vengono controllate ed aggiornate quando richiesto.

2. Misure Tecniche Dettagliate

In aggiunta, di seguito sono indicate misure tecniche specifiche che devono essere eseguite o implementate da Intesa per aiutare a proteggere la privacy e la sicurezza dei dati personali.

Altre misure che possono essere appropriate per proteggere la privacy e la sicurezza dei dati personali trattati da Intesa nell'ambito del Servizio, ma non indicate di seguito o altrove nell'Accordo, devono essere fornite o implementate dal Cliente.

Categoria	Nome abbreviato	Requisiti di Controllo
Monitoraggio sicurezza	Requisiti d'Accesso	I log di sistema e gli eventi sui sistemi che trattano Dati Personali devono essere copiati in un sistema non accessibile all'amministratore di sistema o agli operatori le cui attività vengono registrate.
Monitoraggio sicurezza	Requisiti di monitoraggio	I tool di monitoraggio dei log devono essere utilizzati per analizzare i log sui sistemi che trattano Dati Personali e per rilevare eventuali comportamenti sospetti ed inviare alert.
Monitoraggio sicurezza	Conservazione dei log	I log devono essere conservati per il periodo richiesto dalla legge applicabile.
Monitoraggio sicurezza	Monitoraggio integrità dei file	Implementare il Monitoraggio dell'integrità dei file per identificare modifiche non autorizzate al sistema o ai file di configurazione sui server che elaborano Dati Personali.
Test della Sicurezza e Gestione della Configurazione	Scansione di Vulnerabilità	Eseguire con cadenza mensile le scansioni di vulnerabilità dei sistemi in cui viene eseguito il trattamento dei Dati Personali. Gli scanner saranno aggiornati periodicamente per rilevare le vulnerabilità più recenti.
Test della Sicurezza e Gestione della Configurazione	Test di Penetrazione	Almeno una volta all'anno, condurre test di penetrazione esterni ed interni sui sistemi in cui viene eseguito il trattamento dei Dati Personali. Notare che questo requisito non è soddisfatto mediante l'utilizzo dei test di sicurezza automatizzati e deve essere eseguito tramite un tester di penetrazione.
Test della Sicurezza e Gestione della Configurazione	Scansioni automatizzate delle porte	Eseguire periodicamente le scansioni automatizzate delle porte da Internet su tutti i server in cui viene eseguito il trattamento dei Dati Personali rispetto ad una base di riferimento definita. Le anomalie dovranno generare avvisi ed essere esaminate.
Test della Sicurezza e Gestione della Configurazione	Test Disponibilità Organizzativa	Eseguire le esercitazioni principali della tabella "Red team" almeno una volta all'anno per testare la capacità organizzativa di identificare e ridurre gli attacchi informatici.
Supporto di Backup e dati personali 'Dormienti'	Riutilizzo Supporti di Backup	Cancellare e rimuovere tutti i Dati Personali dai dispositivi di storage di backup in modo tale che non sia possibile accedere o ricreare i Dati Personali, dopo la disattivazione del dispositivo e prima di riutilizzarlo.
Prevenzione perdita dei dati	Blocco Schermo	Configurare i blocchi schermo per limitare l'accesso alle workstation non presidiate in cui sono contenuti Dati Personali.
Prevenzione perdita dei dati	Prevenzione Perdita dei Dati di Rete	Implementare i sensori di rete per aiutare a rilevare e bloccare i tentativi di estrapolazione non autorizzata dei Dati Personali dalla rete.

Categoria	Nome abbreviato	Requisiti di Controllo
Prevenzione perdita dei dati	Limitazione di Accesso ai Dati	Implementare controlli che impediscono agli amministratori di ottenere copie dei Dati Personali trattati sui sistemi gestiti da Intesa.
Prevenzione perdita dei dati	Pseudonimizzazione & Anonimizzazione	Promuovere l'utilizzo della pseudonimizzazione e dell'anonimizzazione dei Dati Personali nelle operazioni.
Prevenzione perdita dei dati	Limitazioni Unità USB	Implementare controlli tecnici progettati per aiutare a prevenire o rilevare e segnalare a livello centrale il trasferimento non autorizzato dei Dati Personali dalle workstation ad unità USB o ad altri supporti esterni.
Prevenzione perdita dei dati	Sicurezza Data Center	Collocare i sistemi che trattano Dati Personali presso strutture con restrizioni sugli accessi al fine di consentire l'accesso solo al personale autorizzato.
Disaster Recovery	Test del Backup	Convalidare periodicamente l'integrità del processo di backup eseguendo i test di ripristino dei dati.
Disaster Recovery	Disaster Recovery	Implementare funzionalità di Disaster Recovery progettate per recuperare le funzionalità del sistema che tratta Dati Personali in un periodo di tempo definito, basato su una valutazione di impatto. Il sito e il sistema di recupero devono avere misure di sicurezza almeno equivalenti alle misure implementate sul sito primario.
Disaster Recovery	Backup dei Dati	Backup dei dati giornaliero su sito geografico differente.
Disaster Recovery	Conservazione dei backup dei dati Offsite	I backup dei dati sono conservati su un sito geografico differente.
Network Management	Filtri Web	Predisporre controlli che filtrino l'accesso Web progettati per bloccare l'accesso a siti Web dannosi da parte di sistemi in cui viene eseguito il trattamento dei Dati Personali.
Network Management	Blocco IP Dannosi	Implementare i controlli progettati per bloccare le comunicazioni di rete verso e da sistemi in cui viene eseguito il trattamento dei Dati Personali con indirizzi IP dannosi (black list) o che consentono l'accesso solo con siti affidabili (whitelist).
Network Management	Prevenzione delle intrusioni Network	Implementare sistemi di prevenzione delle intrusioni sui network che trattano Dati Personali.
Network Management	Segmentazione della Rete	Segmentare le reti in modo tale che i sistemi in cui viene eseguito il trattamento dei Dati Personali si trovino su reti logiche separate o su VLAN con controlli dei firewall, al fine di consentire il traffico solo verso e da fonti autorizzate.
Network Management	Crittografia delle Applicazioni	Crittografare i Dati Personali durante il transito su qualsiasi rete.
Network Management	Host-Based Firewall	Applicare firewalls o filtri d'accesso sui sistemi che trattano Dati Personali, in modo da inibire l'accesso per il traffico che non sia specificatamente autorizzato.
Network Management	Integrità dei Dispositivi di Rete	Riconvalidare le regole del firewall almeno annualmente per i dispositivi che proteggono i sistemi del Cliente gestiti da Intesa in cui viene eseguito il trattamento di dati personali.
Formazione e Intelligence sulle Minacce	Formazione alla Sensibilizzazione sulla Sicurezza	Implementare un programma di sensibilizzazione sulla sicurezza obbligatorio per i dipendenti.

Categoria	Nome abbreviato	Requisiti di Controllo
Formazione e Intelligence sulle Minacce	Management dei fornitori	Implementare un programma di management per I fornitori che trattano I Dati Personali che sia progettato per assicurare l'effettiva correttezza nella scelta dei fornitori, nella implementazione dei contratti, nella supervisione in corso di contratto.
Gestione Identità ID utente e Accesso	Accertamento individuale degli account	Implementare controlli adeguati per garantire l'accertamento individuale degli account.
Gestione Identità ID utente e Accesso	Blocco Account del Sistema Operativo	Implementare i controlli per bloccare attacchi di tipo 'brute force' finalizzati all'individuazione delle password nelle applicazioni in esecuzione nei sistemi in cui viene eseguito il trattamento dei Dati Personali. Ad esempio, bloccare gli account dopo un numero definito di tentativi di accesso non riusciti
Gestione Identità ID utente e Accesso	Riconvalidare gli ID Utente Intesa	Riconvalidare ogni anno le esigenze aziendali per gli ID Utente Intesa e le autorizzazioni associata con accesso ai Dati Personali.
Gestione Identità ID utente e Accesso	Disconnessione automatica dell'applicazione	Disconnettere automaticamente gli utenti dai sistemi in cui viene eseguito il trattamento dei Dati Personali dopo un periodo definito di inattività.
Gestione Identità ID utente e Accesso	Rimozione Client ID	Revocare l'accesso agli ID utente del Cliente con accesso ai dati personali sui sistemi del Cliente gestiti dal Intesa nel più breve tempo possibile non appena cessano le esigenze aziendali.
Gestione Identità ID utente e Accesso	Limitazione Accessi	Limitare l'accesso ai Dati Personali nei file system, nelle condivisioni di rete, nelle applicazioni e nei database utilizzando "access control lists" sui sistemi gestiti da Intesa solo alle persone con esigenze aziendali che richiedono l'accesso.
Gestione Identità ID utente e Accesso	Crittografia dell'accesso di rete	Crittografare tutti gli accessi di rete ai sistemi che memorizzano o in cui viene eseguito il trattamento dei Dati Personali (ad es., non può essere utilizzato nessun protocollo di testo in chiaro come HTTP, FTP o Telnet. I protocolli come RDP e VNC devono essere configurati in modo da utilizzare la crittografia).
Gestione Identità ID utente e Accesso	Crittografia ID File	Crittografare o eseguire l'algoritmo hash su tutti i file di autenticazione nei sistemi in cui viene eseguito il trattamento dei Dati Personali e richiedere i privilegi root o di amministratore per eseguire l'accesso.
Gestione Identità ID utente e Accesso	Lunghezza delle password	Laddove l'autenticazione a più fattori non fosse supportata, richiedere una password di lunghezza minima di 14 caratteri, se supportata, sugli ID utente con accesso ai sistemi che trattano dati personali.
Gestione delle Patch	Tempistica delle Patch	<p>Applicare le patch di sicurezza ai sistemi in cui viene eseguito il trattamento dei Dati Personali durante le finestre di manutenzione regolarmente pianificate. Le finestre di manutenzione devono essere stabilite in base alla seguente pianificazione:</p> <ul style="list-style-type: none"> ● Sistemi che accedono a Internet: almeno una volta ogni 30 giorni. ● Sistemi che non accedono a Internet: almeno una volta ogni 60 giorni.
Gestione delle Patch	Applicazione di Patch alle Applicazioni Gestite da Intesa	Applicare le patch delle applicazioni e del middleware sui sistemi in cui viene eseguito il trattamento dei Dati Personali.

Categoria	Nome abbreviato	Requisiti di Controllo
Gestione delle Patch	Supporto del Software	Verificare che tutte le versioni di software in uso (sistemi operativi, applicazioni, browser, client di posta, middleware e così via) siano attualmente supportati dal relativo fornitore.
Gestione delle Patch	Test del Software	Eseguire il test del nuovo software (inclusi patch, service pack ed altri aggiornamenti) in un ambiente non di produzione prima della promozione alla produzione.
Whitelist di applicazioni/anti-virus/anti-malware	Anti-Virus (Sistemi)	Distribuire software di rilevazione e prevenzione anti-virus/anti-malware su tutti i server gestiti da Intesa in cui viene eseguito il trattamento dei Dati Personali. Periodicamente tale software riceverà, da un'infrastruttura centrale, aggiornamenti delle "reputation-based signatures". Gli eventi rilevati devono essere registrati a livello centrale.
Whitelist di applicazioni/anti-virus/anti-malware	Protezione del Cliente da Phishing	Distribuire controlli di rilevazione e prevenzione basati sulla rete per aiutare a filtrare le email di phishing ed i malware prima che raggiungano un endpoint.
Whitelist di applicazioni/anti-virus/anti-malware	Whitelist delle Applicazioni	Distribuire whitelist delle applicazioni su tutte le workstation in cui viene eseguito il trattamento dei Dati Personali per impedire che su tali workstation venga eseguito software non autorizzato.
Risposta agli Incidenti	Risposta agli Incidenti	Mantenere una capacità di investigazione e reazione agli incidenti relativi all'IT sufficiente per la conformità con le leggi applicabili, incluse quelle che riguardano la notifica delle violazioni dei dati.
Gestione Inventario	Software di Inventario	Mantenere un inventario accurato del software, che includa la versione ed il sistema operativo sottostante, sui sistemi in cui viene eseguito il trattamento dei Dati Personali.