incico spa
advanced integrated engineering

INCICO S.P.A.

Sede Legale: Via Terranuova n.28
Ferrara (FE)
P.I. 00522150382
Sede Operativa: Via Zandonai n.4
Ferrara (FE)

Identificazione del Documento
Modello Organizzativo Privacy Redatto in conformità al D.Lgs 196/03 e s.m.i. E Reg.UE 2016/679

Stato delle edizioni ed aggiornamento
Prima emissione 04.09.2020
Rev.1 26.01.2022
Rev. 2 08.03.2023

Revisione 2	
Ferrara (FE), 08.03.2023	Il l.r. di INCICO S.P.A.  Olivier Severini

www.incico.com

Il presente Documento è di proprietà esclusiva di INCICO S.P.A.. Qualunque divulgazione, riproduzione o cessione di contenuti a

terzi deve essere preventivamente autorizzata da INCICO S.P.A.. Una copia del presente M.O.P. verrà consegnata a chiunque ne faccia richiesta, con motivate ragioni ed in relazione all'instaurarsi di un rapporto che implichi un trattamento di dati personali.

www.incico.com

Indice

www.incico.com

ALLEGATI

All.to A) Analisi e valutazione dei rischi

All.to B) Mansionario Privacy, Banche Dati, Asset Autorizzati, Lista detentori chiavi di accesso, Responsabili del Trattamento ex art. 28 Reg. UE 2016/679

All.to C) Registro delle attività dei trattamenti del Titolare e del Responsabile

All.to D) Piano verifiche GDPR

REGISTRI

RV. Registro Violazioni Data Breach

RF. Registro Formazione GDPR

R.I. Registro Istanze Interessati

MODELLI

Informative al trattamento dei dati personali

Nomina ed istruzioni autorizzati al trattamento

Designazione Data Protection Officer

Designazione Amministratore di Sistema

Contratto di Nomina del Responsabile del Trattamento ex art.Art. 28 Reg.UE 2016/679

Privacy Policy del Sito web

www.incico.com

1. Ambito di applicazione ed efficacia

In conformità a quanto previsto dal D.lgs 196/03 e s.m.i. e dal Reg. UE 2016/679, il presente documento, di seguito denominato Modello Organizzativo Privacy o semplicemente M.O.P., viene redatto allo scopo di delineare il quadro delle misure di sicurezza che INCICO S.P.A. (qui di seguito individuata come il *Titolare*) adotta, o si propone di adottare, nell'ambito del trattamento dei dati personali dei propri dipendenti, clienti, partner commerciali o professionisti che, a vario titolo, collaborano con la stessa.

Allo scopo di implementare il proprio sistema di "Governance della Data Protection", verificare l'efficacia delle procedure e dei processi che garantiscono la disponibilità, l'esclusività, l'integrità e la continuità delle informazioni trattate dal Titolare, nonché al fine di assicurare un livello di sicurezza adeguato al rischio, INCICO S.P.A. ha altresì adottato un "**Manuale delle Contromisure**", da considerarsi parte integrante del presente M.O.P.

Il presente modello disciplina il trattamento, automatizzato e non, di dati personali contenuti in un archivio o destinati a figurarvi, posto in essere dal Titolare e dalle funzioni aziendali a ciò preposte, mediante strumenti sia elettronici, che cartacei.

Il presente M.O.P sostituirà il precedente Documento Programmatico sulla Sicurezza adottato dal Titolare e sarà aggiornato con cadenza annuale.

1.1. Definizioni

Conformemente a quanto previsto dall'art. 4 Reg.UE 2016/679, ai fini del presente M.O.P. si intende per:

«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Si precisa come sia auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative ad una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti ad una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi dii cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente.
«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
«**limitazione del trattamento**»: il contrassegno di dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Si precisa come al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori ed al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche.

www.incico.com

«**pseudonimizzazione**»: il trattamento dei dati personali strutturato in modo tale che i dati stessi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

«**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

«**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

«**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

«**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

«**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

«**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, a che i dati personali che lo riguardano siano oggetto di trattamento.

Si precisa come il consenso debba essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesti l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. Non è configurabile come consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso deve essere applicato a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso deve essere prestato per ciascuna delle stesse. Qualora il consenso dell'interessato sia richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

«**violazione dei dati personali**» c.d. "Data Breach": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (V.Procedura di data breach).

«**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

«**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

«**stabilimento principale**»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha

www.incico.com

sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento, nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del Reg.UE 2016/679;
«**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27 Reg.UE 2016/679, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Reg.UE 2016/679;
«**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.
«**gruppo imprenditoriale**»: gruppo costituito da un'impresa controllante e dalle imprese da queste controllate.
«**trattamento transfrontaliero**»: trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro, oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

1.2. Principi generali

Il Titolare si impegna ad osservare, nel trattamento dei dati personali, i seguenti principi:

Responsabilizzazione: il titolare del trattamento è responsabile dei trattamenti di dati personali dallo stesso posti in essere. In particolare, il titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento alle norme vigenti in materia di privacy, compresa l'efficacia delle misure. Tali misure devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.
Liceità, correttezza e trasparenza: i dati personali sono trattati dal Titolare in modo lecito, corretto e trasparente nei confronti dell'interessato.
Limitazione della finalità: i dati personali sono raccolti dal Titolare per finalità determinate, esplicite e legittime e successivamente trattati in modo che il trattamento non risulti incompatibile con tali finalità. Qualora il Titolare tratti i dati per finalità differenti rispetto a quelle originariamente individuate, lo stesso sarà tenuto ad acquisire nuovamente il consenso dell'interessato.
Minimizzazione dei dati: i dati personali trattati dal Titolare sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Esattezza: il Titolare garantisce che i dati personali raccolti risultino esatti e, se necessario, aggiornati, il Titolare si impegna altresì ad adottare tutte le misure ragionevoli ed adeguate allo scopo di rettificare tempestivamente i dati risultanti inesatti.
Limitazione della conservazione: i dati personali sono conservati dal Titolare in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta

www.incico.com

salva l'attuazione di misure tecniche e organizzative adeguate richieste dal REG.UE 2016/679 a tutela dei diritti e delle libertà dell'interessato.

Integrità e riservatezza: il Titolare garantisce la sicurezza e la protezione dei dati personali trattati, adottando misure tecniche e organizzative adeguate, allo scopo di prevenire, o quanto limitare, il rischio di trattamenti non autorizzati o illeciti nonché la perdita e/o la sottrazione dei dati.

2. Organizzazione della società, tipologia di dati trattati e modalità di trattamento

2.1. Organizzazione della Società

Nomina	
Titolare del Trattamento	INCICO S.P.A.
Data Protection Officer	IQC S.r.l. in persona dell'Avv. Barbara De Cillis
Amministrazione di Sistema	V. Nomina Amministratore di Sistema
Autorizzati al Trattamento	V. allegato B) - Mansionario
Responsabili del Trattamento	V. allegato B) – Responsabili del trattamento

2.2. Tipologia di dati trattati

Tipologia di dati	Clienti/Fornitori		Personale Dipendente		Candidati off. lavoro	
	SI	NO	SI	NO	SI	NO
Dati anagrafici						
Nome e Cognome / Ragione Sociale	☒	☐	☒	☐	☒	☐
Data e luogo di nascita	☐	☒	☒	☐	☒	☐
Codice fiscale/P.IVA	☒	☐	☒	☐	☒	☐
Dati di contatto						
Indirizzo abitazione / Sede Legale	☒	☐	☒	☐	☒	☐
Email personale	☐	☒	☒	☐	☒	☐
Email aziendale	☒	☐	☒	☐	☐	☒
Recapiti telefonici aziendali	☒	☐	☒	☐	☐	☒
Recapiti telefonici personali	☐	☒	☒	☐	☒	☐
Dati giudiziari						
Dati giudiziari (sede civile)	☐	☒	☒	☐	☐	☒
Dati relativi a condanne o reati	☐	☒	☐	☒	☐	☒
Altre tipologie di dati comuni						
Coordinate bancarie	☒	☐	☒	☐	☐	☒
Estremi documento di identità	☐	☒	☒	☐	☒	☐
Particolari categorie di dati						

www.incico.com

Origine razziale o etnica	☐	☒	☐	☒	☐	☒
Dati biometrici	☐	☒	☐	☒	☐	☒
Dati genetici	☐	☒	☐	☒	☐	☒
Dati relativi alla geolocalizzazione	☐	☒	☐	☒	☐	☒
Dati relativi allo stato di salute	☐	☒	☒	☐	☒	☐
Dati relativi all'appartenenza sindacale	☐	☒	☒	☐	☐	☒
Dati relativi alle opinioni politiche	☐	☒	☒	☐	☐	☒
Dati relativi alle convinzioni religiose	☐	☒	☒	☐	☐	☒
Dati relativi all'orientamento sessuale	☐	☒	☐	☒	☐	☒
Altre tipologie di dati						
Foto	☐	☒	☒	☐	☒	☐
Video	☐	☒	☐	☒	☐	☒
Immagini acquisite tramite impianto di videosorveglianza	☐	☒	☐	☒	☐	☒
Targa veicolo	☐	☒	☐	☒	☐	☒
Dati relativi a familiari	☐	☒	☒	☐	☐	☒
Dati di profilazione	☐	☒	☐	☒	☐	☒

2.3. Modalità di trattamento

2.3.1. Modalità di trattamento dei dati del personale dipendente

Il trattamento dei dati del personale dipendente, la cui base giuridica è individuata nell'esecuzione del rapporto di lavoro (Art. 6 lett.b e c) e 9 lett.b) Reg. UE 2016/679), è posto in essere previo rilascio dell'informativa al trattamento dei dati e sottoscrizione, per ricevuta della stessa, da parte del lavoratore.

Le funzioni aziendali preposte al trattamento di dati personali, all'atto dell'assunzione ricevono:

a) l'informativa al trattamento dei dati personali

b) la lettera di nomina ad autorizzato del trattamento dei dati personali e brevi istruzioni operative

d) il regolamento per l'utilizzo delle postazioni informatiche

L'informativa al trattamento dei dati, rinnovata alla luce delle disposizioni introdotte dal Reg.UE 2016/679, è stata inoltre affissa nella bacheca aziendale di INCICO S.P.A..

Il trattamento dei dati del personale dipendente, più dettagliatamente descritto nel Registro delle Attività dei Trattamenti del Titolare, è affidato all'Ufficio Amministrazione il quale provvede agli adempimenti necessari all'instaurazione ed alla gestione del rapporto di lavoro.

Il Titolare, nel rispetto delle disposizioni dettate dal Reg.UE 2016/679 e dalla L 300/70, ha configurato i propri sistemi informativi riducendo al minimo il trattamento di dati personali dei lavoratori. In tal modo, il trattamento di tali dati è escluso quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi.

Il Titolare ha inoltre adottato misure di sicurezza a garantire che:

- le comunicazioni personali riferibili esclusivamente a singoli lavoratori avvengano con modalità tali da escluderne l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali autorizzati;
- siano impartite chiare istruzioni agli autorizzati in ordine al trattamento dei dati personali del personale dipendente;

www.incico.com

- sia prevenuta l'acquisizione e riproduzione, da parte di soggetti non autorizzati, di dati personali trattati elettronicamente e/o di documenti contenenti informazioni personali.

2.3.2. Modalità di trattamento dei dati di clienti e fornitori

Il trattamento dei dati di clienti e fornitori è posto in essere previo rilascio dell'informativa al trattamento dei dati redatta ai sensi e per gli effetti dell'art. 13 Reg.UE 2016/679, reperibile e visionabile da ciascun interessato sul sito web di Incico. A tali fini, è stato inserito apposito link nel disclaimer in calce agli indirizzi e-mail del personale dipendente.

Qualora il Titolare, e per esso la funzione aziendale proposta al trattamento dei dati, intenda trattare i dati personali per finalità ulteriori e diverse da quelle per le quali i dati siano stati originariamente raccolti, provvederà ad informare l'interessato ed acquisire nuovamente il consenso del medesimo.

La tipologia di dati raccolti, le finalità e la durata del trattamento risultano più dettagliatamente specificate nel Registro delle Attività dei Trattamenti del Titolare.

2.3.3. Modalità di trattamento dei dati raccolti tramite ricezione dei c.v.

Conformemente a quanto previsto dall'art.111 bis del D.lgs 196/03 e s.m.i., qualora il trattamento abbia ad oggetto curriculum vitae spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione del rapporto di lavoro, il Titolare, e per esso l'autorizzato o la funzione aziendale preposta al trattamento, trasmette all'interessato l'informativa al trattamento dei dati personali in occasione del primo contatto dell'interessato successivo alla ricezione del cv ovvero in occasione della fissazione del colloquio di lavoro. La suddetta informativa al trattamento dei dati personali è reperibile e visionabile dall'interessato sul sito web di Incico. A tali fini, è stato inserito apposito link nel disclaimer in calce agli indirizzi e-mail del personale dipendente.

2.3.4. Modalità di trattamento dei dati degli Utenti

Il Titolare ha provveduto a pubblicare nel proprio Sito web la privacy & cookie policy allo scopo di fornire agli Utenti le informazioni in merito alle modalità di trattamento dei dati dagli stessi forniti.

2.4. Modalità di trattamento dei dati non ottenuti presso l'interessato

Qualora il trattamento abbia ad oggetto dati trasmessi da terzi, ossia non raccolti direttamente presso l'interessato, il Titolare, e per esso l'autorizzato o la funzione aziendale preposta al trattamento, trasmette all'interessato l'informativa al trattamento dei dati personali:

- entro un termine ragionevole dall'ottenimento dei dati – massimo di un mese – in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- qualora i dati siano destinati alla comunicazione con l'interessato, al momento della prima comunicazione con l'interessato;
- in occasione della prima comunicazione dei dati da parte dell'interessato, qualora il trattamento sia finalizzato a consentire la comunicazione con l'interessato medesimo ovvero qualora sia prevista la comunicazione dei dati personali ad un soggetto terzo.

3. Base giuridica del trattamento

3.1. Trattamento di dati personali comuni

Il Trattamento dei dati personali da parte del Titolare ex art.6 Reg.UE 2016/679 è fondato su una delle basi giuridiche di seguito indicate, risultanti, per i singoli trattamenti, dal Registro delle Attività dei Trattamenti.

a) consenso al trattamento di tali dati personali, per una o più specifiche finalità.

www.incico.com

b) esecuzione del contratto, di cui l'interessato è parte od esecuzione di misure precontrattuali adottate su richiesta dello stesso.
c) adempimento di un obbligo legale al quale è soggetto il Titolare del Trattamento.
d) salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Tale base giuridica NON è impiegata dal Titolare.
e) esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Tale base giuridica NON è impiegata dal Titolare.
f) perseguimento di un legittimo interesse del Titolare o di terzi. Si precisa come l'impiego di tale base giuridica richieda una attenta indagine di bilanciamento degli interessi rispettivamente del Titolare e dell'interessato.

In caso di nuovi trattamenti di dati personali, ulteriori rispetto a quelli posti in essere allo stato attuale, gli autorizzati sono tenuti a rivolgersi al Titolare allo scopo di verificare la legittimità, la proporzionalità e le finalità del trattamento ed individuare, conseguentemente, la corretta base giuridica dello stesso.

3.2. Trattamento di particolari categorie di dati

Premesso che, ai sensi dell'art 9 Reg. UE 2016/679, rientrano nella definizione di "particolari categorie di dati" i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco l'interessato, i dati relativi alla salute o alla vita sessuale nonché i dati relativi all'orientamento sessuale dell'interessato, il trattamento avente ad oggetto "particolari categorie di dati" è posto in essere dal Titolare in forza di una delle basi giuridiche di seguito indicate risultanti, per i singoli Trattamenti dal Registro delle Attività dei Trattamenti.

a) consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, prestato dall'Interessato mediante sottoscrizione dell'informativa al Trattamento dei dati personali
b) assolvimento degli obblighi ed esercizio dei diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale
c) tutela di un interesse vitale dell'interessato a condizione che l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso
d) trattamento avente ad oggetto dati personali resi manifestamente pubblici dall'interessato
e) accertamento, esercizio o difesa di un diritto in sede giudiziaria
f) finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale
g) archiviazione per pubblico interesse, ricerca scientifica o a fini statistici, purché siano predisposte misure tecniche ed organizzative che assicurino il rispetto del principio di minimizzazione dei dati.

In caso di nuovi trattamenti di dati personali, ulteriori rispetto a quelli posti in essere allo stato attuale, gli autorizzati sono tenuti a rivolgersi al Titolare ed al Data Protection Officer, allo scopo di verificare la legittimità, la proporzionalità e le finalità del trattamento ed individuare, conseguentemente, la corretta base giuridica dello stesso.

www.incico.com

4. Finalità del Trattamento e periodo di conservazione

4.1. Finalità del Trattamento

Il Titolare, nel rispetto dei principi di cui al P.to 2) del presente M.O.P. tratta dati personali per le finalità di seguito indicate, analiticamente descritte nel Registro delle Attività dei Trattamenti del Titolare alla voce "finalità".

Conclusione ed esecuzione di rapporti contrattuali con clienti, fornitori e partner commerciali. La descritta finalità include il trattamento dei dati comuni (anagrafica e recapiti di contatto) necessari alla conclusione ed esecuzione degli accordi negoziali con clienti, fornitori e partner commerciali nonché a gestire la relativa fatturazione.
Valutazione e accettazione di un fornitore e partner commerciale. La descritta finalità include il trattamento di dati necessari alla valutazione ed all'accettazione di fornitori e partner commerciali.
Sviluppo e miglioramento di prodotti e/o servizi. La descritta finalità include il trattamento di dati necessari allo sviluppo ed al miglioramento di prodotti e/o servizi del Titolare, ricerca e sviluppo.
Esecuzione dei processi aziendali, gestione interna e reporting gestionale. La descritta finalità include il trattamento dei dati personali necessari la gestione delle risorse aziendali, la conduzione di audit ed indagini, finanza e contabilità, l'implementazione di controlli aziendali, la consulenza legale e la gestione delle controversie.
Esecuzione del contratto di lavoro. La descritta finalità include il trattamento dei dati personali comuni e particolari categorie di dati relativi al personale dipendente. Si precisa come, in conformità a quanto previsto dall'Autorizzazione n. 1/2016 (Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro), il trattamento dei dati sensibili dei lavoratori è posto in essere dal Titolare unicamente se indispensabile per le seguenti finalità:

Adempiere ed esigere l'adempimento di specifici obblighi, eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi anche aziendali ed in particolare, ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica.
Tenere la contabilità e corrispondere stipendi, assegni, premi od altri emolumenti.
Salvaguardare la vita o l'incolumità fisica del lavoratore o di un terzo.
Far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi.
Esercitare il diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia.
Adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale.
Garantire le pari opportunità nel lavoro.
Perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza

www.incico.com

sindacale ai datori di lavoro.

Si precisa altresì come, il trattamento potrà avere ad oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, ed in particolare:

- nell'ambito dei dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, i dati concernenti la fruizione di permessi e festività religiose o di servizi di mensa;

- nell'ambito dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale, i dati concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali (sempre che il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pubbliche iniziative, nonché i dati inerenti alle trattenute per il versamento delle quote di servizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;

- nell'ambito dei dati idonei a rivelare lo stato di salute, i dati raccolti e trattati in riferimento a invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psico-fisica a svolgere determinate mansioni, all'appartenenza a determinate categorie protette, nonché i dati contenuti nella certificazione sanitaria attestante lo stato di malattia, anche professionale dell'interessato, o comunque relativi anche all'indicazione della malattia come specifica causa di assenza del lavoratore.

Conformità alla legge. La descritta finalità include il trattamento dei dati personali necessari all'adempimento di obblighi legali ai quali è soggetto il Titolare del Trattamento.

4.2. Periodo di conservazione dei dati personali

Fatti salvi gli obblighi di legge in materia di conservazione dei dati personali, i dati trattati dal Titolare sono conservati per il **periodo di tempo strettamente necessario al perseguimento delle finalità sottese al trattamento medesimo**.

Il periodo di conservazione di ciascuna tipologia di dati risulta indicato nel Registro delle Attività di Trattamento (Allegato C). Al termine del trattamento i dati personali saranno eliminati o resi anonimi.

www.incico.com

Riepilogo dei dati trattati, tipologia, finalità, base giuridica del trattamento, modalità di rilascio dell'informativa ed eventuale acquisizione del consenso

Categoria di interessati e tipologia di dati	Finalità	Base giuridica	Modalità di rilascio dell'informativa ed eventuale acquisizione del consenso
Personale dipendente (dati comuni e particolari)	Instaurazione e gestione del rapporto di lavoro, adempimento dei connessi obblighi di legge	Art. 6 c.1 lett. b) e c) Art.9 c.2 lett. b) Reg.UE 2016/679	□ Consegna dell'informativa al dipendente e sottoscrizione per ricevuta □ Affissione nella bacheca aziendale
Clienti e fornitori (dati comuni)	Gestione del rapporto contrattuale ed adempimento dei connessi obblighi di legge	Art. 6 c.1 lett. b) e c) Reg.UE 2016/679	□ Informative Clienti e Fornitori pubblicate sul sito web. Informativa breve con link presente nel disclaimer in calce agli indirizzi e-mail del personale dipendente
Candidati alle offerte di lavoro	Instaurazione del rapporto di lavoro	Art. 111 bis D.lgs 196/03 e s.m.i. Reg.UE 2016/679	□ Informative CV pubblicata sul sito web. Informativa breve con link presente nel disclaimer in calce agli indirizzi e-mail del personale dipendente
		Art. 6 c.1 lett.b) Reg.UE 2016/679 (candidature ad offerte di lavoro tramite sito web)	□ Privacy Policy pubblicata sul sito internet
Utenti del sito web	Navigazione e presa visione dei contenuti presenti sul sito web	Art. 6 c.1 lett.b) Reg.UE 2016/679	□ Privacy Policy pubblicata sul sito internet

www.incico.com

5. Valutazione dell'applicabilità degli art. 30, 35, 37 Reg. UE 2016/679

In ragione della tipologia di trattamento posto in essere dalla Titolare, si ritiene che la stessa ALLO STATO ATTUALE:

- **NON sia** soggetta all'obbligo di eseguire una **Valutazione di Impatto** sulla protezione dei dati personali, ai sensi e per gli effetti dell'art. 35 Reg.UE 2016/679.
- **SIA** soggetta all'obbligo di tenuta dei **registri delle attività di trattamento**, ai sensi e per gli effetti dell'art. 30 Reg.UE 2016/679. Allo scopo di adempiere compiutamente alla disciplina vigente in materia di protezione dei dati personali, INCICO S.P.A. ha predisposto il Registro delle Attività dei Trattamenti del Titolare e del Responsabile, allegato al presente M.O.P. E' compito del Titolare verificare l'efficacia delle procedure poste a presidio del sistema di data governance, curando l'aggiornamento del Registro delle Attività dei Trattamenti.
- **NON** Sia soggetta all'obbligo di Designazione del Data Protection Officer ai sensi e per gli effetti dell'art. 37 Reg.UE 2016/679. Al fine di garantire l'efficacia del sistema privacy adottato INCICO S.P.A. ha provveduto alla **designazione volontaria** di un proprio Data Protection Officer.

6. Distribuzione dei compiti e delle responsabilità – Mansionario Privacy

Il Mansionario Privacy allegato al presente M.O.P. (All.to B.1) contiene l'indicazione delle funzioni aziendali preposte al trattamento dei dati, la definizione delle rispettive aree di competenza e l'individuazione dei soggetti terzi a cui il Titolare trasmette/comunica dati personali. In tale modo, in conformità al principio di accountability introdotto dal Reg. UE 2016/679, il Titolare dispone di un quadro chiaro di "*chi fa cosa*" nell'ambito del trattamento dei dati personali.

6.1. Data Protection Officer (RPD)

Previa verifica dei requisiti di esperienza, capacità ed affidabilità, il Titolare ha nominato un proprio Data Protection Officer (v. All.To – Nomina del Data Protection Officer), al quale ha affidato i seguenti compiti:

- informare e fornire consulenza al Titolare del trattamento (o al responsabile del trattamento) ed al personale dipendente autorizzato al trattamento, in merito agli obblighi derivanti dal Reg.UE 2016/679, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali;
- sorvegliare l'osservanza del Reg.UE 2016/679, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali nonché delle politiche adottate dal titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 Reg.UE 2016/679;
- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 Reg.UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- predisporre, anche in contraddittorio con il Titolare del Trattamento, un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, atto a verificare l'efficacia delle misure di sicurezza adottate;
- comunicare prontamente e per iscritto al Titolare il verificarsi di una violazione dei dati personali ai sensi e per gli effetti degli artt. 33 s.s. Reg. UE 2017/679 e, qualora se ne ravvisi l'obbligo, coadivuare il Titolare

www.incico.com

nelle operazioni di notifica all'Autorità Garante ed eventuali comunicazioni ai soggetti interessati, così come prescritto dalla relativa "Procedura di Data Breach";

- riscontrare le istanze degli interessati, dando seguito alla "Procedura di Riscontro delle istanze degli interessati, predisposta dal Titolare.

6.2. Amministratore di Sistema (A.d.S.)

Il Titolare nel pieno rispetto del provvedimento del Garante per la Protezione dei dati Personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*", (G.U. n. 300 del 24 dicembre 2008), previa verifica dei requisiti di esperienza, capacità ed affidabilità, ha provveduto a nominare un proprio Amministratore di Sistema (v. All.to – nomina A.d.S.), al quale ha affidato i seguenti compiti:

- rispettare e vigilare sul rispetto delle misure di sicurezza indicate nel Modello Organizzativo Privacy e nel Manuale delle Contromisure predisposto dal Titolare;
- proteggere ogni elaboratore (server o client di rete e macchine stand-alone) da accessi esterni non autorizzati e da virus informatici, approntando adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali, aggiornate alla luce delle nuove tecnologie fruibili sul mercato (firewall, proxy, antivirus ecc.);
- assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery) (modalità, periodicità e recupero), assicurando la correttezza e la conservazione delle stesse in un luogo sicuro, il cui accesso sia inibito a soggetti non autorizzati, ed adatto, ovvero protetto e possibilmente ignifugo;
- gestire gli user-profile (credenziali di autenticazione), assegnando ad ogni autorizzato al trattamento il relativo user-id ed una "prima" password d'accesso, consentendo al contempo all'autorizzato (tramite funzione o programma appropriato o presidio) di poter modificare autonomamente la propria password;
- verificare che gli autorizzati provvedano alla modifica della propria password, con cadenza trimestrale, qualora il trattamento abbia ad oggetto particolari categorie di dati, con cadenza semestrale per i restanti trattamenti;
- sospendere gli user-profile (user-id & password) degli autorizzati al Trattamento che si assentino dalle attività lavorative per un periodo superiore 6 mesi (6 mesi + 1g) e cancellare definitivamente gli user-profile degli autorizzati che si assentino per un periodo superiore a 12 mesi (12 mesi + 1g). Si precisa come gli user-profile (e relativi user-id) cancellati non potranno più essere riutilizzati.

CAUTELE PER ASSICURARE LA SEGRETEZZA DELLE CREDENZIALI DI ACCESSO

Ogni autorizzato deve essere reso edotto che le credenziali di autorizzazione sono personali, non devono essere comunicate a nessuno, non devono essere trascritte.

CARATTERISTICHE DELLA PASSWORD

La password deve essere composta da almeno 12 caratteri di cui almeno un carattere speciale, una lettera minuscola ed una maiuscola, non deve essere uguale ad una delle cinque password precedentemente utilizzate, non deve contenere riferimenti agevolmente riconducibili all'interessato, né consistere in nomi noti, anche di fantasia.

MODALITA' DI RILASCIO DELLE CREDENZIALI DI AUTORIZZAZIONE

L'A.d.S., al momento dell'attivazione, comunica all'autorizzato la propria credenziale e la password provvisoria che quest'ultimo provvederà a modificare.

- adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) da parte dell'Amministratore di Sistema ai sistemi di elaborazione ed agli archivi elettronici. Si precisa come le registrazioni (*access log*) debbano avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste,

www.incico.com

debbano comprendere i riferimenti temporali, la descrizione dell'evento che le ha generate e debbano essere conservate per un congruo periodo, non inferiore a sei mesi;

- partecipare alle riunioni del Team di crisi in caso di data breach, osservando la procedura predisposta dal Titolare;
- organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, la verifica di eventuali tentativi di accesso non autorizzati al sistema provenienti da soggetti terzi quali accesso abusivo al sistema informatico o telematico, frode informatica, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici, avvisando prontamente il Titolare o il Responsabile del Trattamento.

E' compito dell'Amministratore di Sistema monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dei dati di cui sopra, mantenendo aggiornati i supporti hardware e software e, se del caso, comunicando al Titolare tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in relazione alla tipologia e quantità dei dati personali trattati.

6.3. Autorizzati al Trattamento dei dati

Il Titolare ha provveduto a designare quali "Incaricati/Autorizzati al Trattamento dei dati" le funzioni aziendali preposte al trattamento dei dati personali (V. All.to Nomina ad Autorizzato del Trattamento dei dati).

Nelle lettere di nomina è indicata l'area di trattamento consentito a ciascun autorizzato al quale vengono consegnate le istruzioni per il trattamento dei dati personali.

Istruzioni generali

- Verificare, con la massima attenzione, l'esattezza dei dati personali raccolti, la pertinenza e la non eccedenza degli stessi; trattare i dati personali secondo correttezza ed in modo lecito provvedendo, quando risulta necessario, all'aggiornamento degli stessi.
- Accedere ai soli dati personali la cui conoscenza risulti strettamente indispensabile all'adempimento delle proprie mansioni, in caso di dubbio, rivolgersi direttamente al Titolare.
- Non comunicare dati personali a mezzo telefono, e-mail o fax qualora non si abbia la certezza dell'identità del destinatario. Prima di procedere alla trasmissione dei dati personali a terzi, verificare che la terza parte sia stata nominata, mediante accordo contrattuale, Responsabile del Trattamento dei Dati ex art. 28 Reg. UE 2016/679, in caso contrario rivolgersi al Titolare.
- Segnalare al Titolare la creazione di nuove banche dati personali ed eventuali criticità rilevate nel corso del trattamento. Rivolgersi al Titolare e/o al Data Protection Officer in caso di dubbio sulle modalità o sulle finalità del trattamento.
- **Comunicare prontamente al Titolare ed all'Amministratore di Sistema eventuali violazioni/perdita di dati** (virus, furto o smarrimento di un dispositivo portatile contenente dati personali...).
- Partecipare alle iniziative formative in materia di trattamento dei dati organizzate dal Titolare.

Rilascio dell'informativa al trattamento dei dati ed acquisizione del consenso

- Per l'acquisizione dei dati personali forniti direttamente dall'interessato: in occasione del primo contatto rendere all'interessato l'informativa al trattamento dei dati personali e richiedere il conferimento del consenso per iscritto (qualora il trattamento dei dati sia fondato sul consenso dell'interessato), tramite i moduli messi a disposizione dal Titolare, verificando che l'informativa impiegata sia pertinente allo specifico trattamento effettuato e completa in ogni sua parte.

www.incico.com

- Per l'acquisizione dei dati personali trasmessi tramite curriculum vitae, rendere l'informativa all'interessato in occasione del primo contatto utile (es. fissazione del colloquio).
- Archiviare le informative raccolte in modo che le stesse risultino, all'occorrenza, prontamente reperibili.

Custodia ed archiviazione dei supporti

- Prelevare dagli archivi i soli supporti o documenti cartacei contenenti dati personali necessari allo svolgimento delle mansioni lavorative e riporre i supporti o documenti cartacei negli archivi al termine delle operazioni di trattamento. I supporti e documenti cartacei contenenti dati personali devono essere controllati e custoditi, in modo appropriato, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento.
- In caso di allontanamento, anche temporaneo, dal posto di lavoro, è necessario identificare un luogo sicuro di custodia dei predetti supporti che offra sufficienti garanzie di protezione da accessi non autorizzati (un armadio, un cassetto o un classificatore chiuso a chiave); ove si utilizzi un contenitore chiuso a chiave, di qualunque natura, occorre accertarsi che le chiavi siano in possesso di incaricati autorizzati.
- Non lasciare incustoditi i supporti contenenti dati personali ed accertarsi che un visitatore od un terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) qualora entri in ufficio, anche se non invitato o per cause accidentali, non possa venire a conoscenza dei contenuti di documenti contenenti dati personali.
- Limitare a quanto strettamente necessario il numero di copie dei supporti e dei documenti cartacei, mantenendo una traccia scritta delle predette copie e degli incaricati o soggetti terzi cui le copie sono state inviate.
- Qualora si utilizzino stampanti o scanner condivisi, non adiacenti alla postazione lavorativa, provvedere a ritirare tempestivamente i documenti contenenti dati personali stampati, sincerandosi di non aver dimenticato alcuna copia.
- Qualora non sia possibile provvedere personalmente alla consegna di documenti o supporti contenenti dati personali gli stessi dovranno essere spediti con modalità di spedizione che consentano un continuo tracciamento ed offrano elevate garanzie di sicura consegna al destinatario.
- Distruggere, sincerandosi di aver reso inutilizzabili/illeggibili eventuali copie dei supporti non riuscite correttamente.

Utilizzo del personal computer e gestione delle password

- Non lasciare incustodito ed accessibile il proprio personal computer durante una sessione di trattamento. Anche in ipotesi di breve assenza, dovrà essere attivato lo *screen saver* con password di sistema.
- La password deve essere composta da almeno **12 caratteri** di cui almeno un carattere speciale, una lettera minuscola ed una maiuscola, non deve essere uguale ad una delle cinque password precedentemente utilizzate, non deve contenere riferimenti agevolmente riconducibili all'interessato, né consistere in nomi noti, anche di fantasia.
- Provvedere a modificare la password non appena viene consegnata dall'Amministratore di Sistema e successivamente, ogni **24 mesi** nonché, immediatamente, nel caso in cui si abbia il sospetto che terzi non autorizzati siano venuti a conoscenza della stessa.
- Conservare la segretezza della password e della credenziale di autenticazione (*username*). Nome utente e password non devono essere, per alcun motivo, comunicate a terzi siano essi soggetti esterni o

www.incico.com

appartenenti all'organizzazione aziendale.

Periodicamente e con cadenza almeno annuale, il Titolare procede ad aggiornare l'area dei dati personali a cui gli incaricati sono autorizzati ad accedere e l'area dei trattamenti che gli stessi sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

6.4. Interventi formativi – formazione iniziale e formazione continua

Sono previsti interventi formativi rivolti agli autorizzati del trattamento al fine di renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali che appaiono più rilevanti avuto riguardo dell'attività svolta dagli autorizzati e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati e misure disponibili per prevenire eventi dannosi;
- modalità di aggiornamento in materia di misure di sicurezza adottate dal Titolare.

Tali interventi formativi hanno luogo in occasione dell'instaurazione del rapporto lavorativo, in presenza di cambiamenti di mansioni ovvero della introduzione di nuovi significativi strumenti che implichino modifiche rilevanti rispetto al trattamento dei dati personali.

Degli interventi formativi viene redatto documento, allegato al presente M.O.P. recante l'indicazione del tipo di evento, della durata e delle risorse aziendali che vi hanno partecipato (All.To B.).

6.5. Responsabili del trattamento

Il Titolare ha provveduto a censire le terze parti alle quali INCICO S.P.A. comunica o trasmette dati personali, contrattualizzando il relativo rapporto (V.all.To B.).

Le terze parti nominate Responsabili del Trattamento dovranno fornire contrattualmente le seguenti garanzie:

a) Modalità di trattamento: il Responsabile si obbliga a trattare i dati personali unicamente su istruzione documentata del Titolare del trattamento;
b) Obbligo di riservatezza: Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) Adozione delle misure di sicurezza: il Responsabile garantisce di aver adottato all'interno della propria organizzazione le misure di sicurezza adeguate richieste ai sensi dell'articolo 32 Reg. UE 2016/679;
d) Nomina "sub-responsabile": il Responsabile si obbliga a non ricorrere ad un altro responsabile senza previa autorizzazione scritta del Titolare;
e) Riscontro delle istanze degli interessati: il Responsabile si impegna ad assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
f) Data Breach, il Responsabile tenuto conto della natura del trattamento e delle informazioni a propria disposizione, si impegna ad assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di notifica delle violazioni dei dati personali.
g) Termine del rapporto: il Responsabile si obbliga a cancellare o restituire al titolare, ad insindacabile scelta di quest'ultimo, i dati personali al termine della prestazione dei servizi relativi al trattamento. Il Responsabile si obbliga altresì a cancellare le copie dei dati eventualmente esistenti.
f) Garanzie ulteriori: Il Responsabile si obbliga a mettere a disposizione del Titolare del trattamento tutte le

www.incico.com

informazioni necessarie a dimostrare il rispetto degli obblighi derivanti dalla sottoscrizione dell'accordo negoziale di nomina, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, eventualmente poste in essere dal Titolare o da un altro soggetto da questi incaricato. Il Responsabile si impegna infine ad informare immediatamente il Titolare qualora ritenga che un'istruzione fornita dal Titolare violi il la normativa vigente in materia.

Il modello dell'accordo contrattuale, integrabile in ragione delle peculiarità dello specifico rapporto negoziale, è allegato al presente Modello Organizzativo (V. All.to Contratto di nomina a Responsabile del Trattamento dei Dati).

www.incico.com

7. Analisi e valutazione dei rischi

Il Titolare ha provveduto ad eseguire una l'analisi dei rischi (All.to B) che incombono sui dati personali e di conformità alla normativa vigente in materia di protezione dei dati personali, nella sede di INCICO S.P.A., allo scopo di individuare ed adottare, tenuto conto dei costi di attuazione, della natura, dell'oggetto del contesto e delle finalità del trattamento, nonché del rischio di gravità e probabilità del rischio per i diritti degli interessati, le misure di sicurezza tecniche ed organizzative adeguate allo scopo di ridurre i rischi di distruzione, perdita dei dati, accesso o divulgazione non autorizzata, accidentale o illecita, dei dati personali dallo stesso trattati.

I rischi individuati nell'All.to A) (Analisi dei Rischi) e nel Manuale delle Contromisure sono stati classificati nelle seguenti categorie:

- rischi “specifici”
- rischi per l'integrità e la riservatezza dei dati
- rischi per la disponibilità dei dati
- rischi di trattamento illecito o non conforme alle finalità del trattamento

7.1. Rischi specifici

Nella categoria dei rischi specifici sono state esaminate quelle minacce che generalmente non trovano una valida protezione nei sistemi di difesa classici, quali le minacce derivanti dalla collocazione territoriale della sede aziendale (eventi atmosferici avversi) e quindi dall’ubicazione dei luoghi in cui vengono custoditi i dati e svolte le diverse operazioni di trattamento.

La sede di INCICO S.P.A. è ubicata a Ferrara Via Zandonai n.4, in una fascia territoriale geografica che risulta classificata tra le zone a medio (3) rischio di pericolosità sismica.

Nella zona limitrofa alle sedi non risultano presenti importanti vie d’acqua che potrebbero esondare nelle vicinanze né in prossimità di punti nodali chiave per i collegamenti con la sede.

Non risultano insediamenti di impianti industriali o altre installazioni di aziende che svolgono attività pericolose nelle immediate vicinanze.

In generale non risultano quindi rischi specifici prevedibili o probabili, correlati alla ubicazione geografica del centro di elaborazione dei dati che richiedano particolari cautele rispetto a quanto indicato in seguito.

7.2. Integrità dei dati

Nell’esame dei rischi per l'integrità dei dati sono stati valutati:

□ rischi accidentali legati al malfunzionamento di apparecchiature hw e sw;

□ rischi legati a condotte involontarie/accidentali/errate da parte di autorizzati (involontaria sovrascrittura o eliminazione di dati personali);

□ rischi legati a condotte di carattere intenzionale (sottrazione, divulgazione e/o diffusione non autorizzata di dati personali da parte del dipendente infedele);

□ rischio di accesso abusivo a sistema informatico (Art. 615 ter c.p.) e minacce derivanti dalla diffusione di virus e programmi pericolosi veicolati da supporti infettati provenienti da dipendenti, da collaboratori senza l’autorizzazione del titolare o da terzi, tramite file scambiati in rete ovvero tramite file ricevuti con posta elettronica.

□ rischi derivanti dall'accesso a dati personali in ragione di un profilo di autorizzazione di incaricato non aderente al ruolo assegnato o conseguente all’attribuzione di “privilegi” di accesso eccessivi, rischio causato da “inferenza” (accesso ad informazioni che consentono, correlate tra loro, di giungere alla conoscenza indiretta dei dati), rischio

www.incico.com

causato dall'utilizzo dei privilegi di "amministratori di sistema", rischi causati dall'accesso a dati personali tramite sistemi di collegamento remoto.

7.3. Disponibilità dei dati

In tale categoria di rischi è stata esaminata l'eventualità che le informazioni non siano disponibili a causa di:

□ anomalie, errori nella procedura di back up dei dati, malfunzionamento hardware (guasti alle unità di elaborazione, di memorizzazione o di trasmissione), dimensionamento non sufficiente delle risorse tecnologiche deputate alla trasmissione ed alla memorizzazione, danneggiamento o manomissione delle attrezzature e/o delle connessioni.

Allo scopo di minimizzare il rischio di perdita di dati, assicurare su base permanente l'integrità, la disponibilità e la resilienza dei sistemi informativi nonché la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali e di business in caso di incidente fisico o tecnico, il Titolare ha adottato **procedure di back-up e di disaster recovery,** allegate al Manuale delle Contromisure, cui si rinvia.

7.4. Trattamento illecito o non conformi alle finalità del trattamento

Il rischio di trattamento illecito è causato dal mancato rilascio dell'informativa al trattamento dei dati e/o dalla mancata acquisizione del consenso (qualora il trattamento si fondi su tale base giuridica) e/o dall'impiego dei dati per finalità diverse da quelle per le quali i dati medesimi risultano essere stati raccolti.

All'esito dell'analisi di conformità alla normativa vigente è emerso quanto segue:

Adempimento/Misura di sicurezza	Normativa di riferimento	Adottata/non adottata
Il Titolare ha uniformato la propria politica aziendale ai principi vigenti in materia di protezione dei dati personali allo scopo di garantire che i dati siano trattati in modo lecito, corretto, per finalità determinate e che gli stessi siano conservati per il periodo di tempo strettamente necessario al perseguimento delle finalità per le quali sono stati raccolti.	Artt. 5-6 Reg. UE 2016/679	☑
Il Titolare ha individuato modalità di raccolta "granulare" del consenso degli interessati, laddove il trattamento si fondi su tale base giuridica, allo scopo di garantire che il consenso sia "informato" e liberamente prestato.	Art. 7 Reg. UE 2016/679	☑
Il Titolare ha individuato i trattamenti aventi ad oggetto "particolari categorie di dati", prevedendo per questi l'adozione di rinforzate misure di sicurezza. In particolare, il Titolare ha definito accessi profilati ai sistemi informativi e misure di custodia di documenti cartacei e supporti allo scopo di limitare il trattamento di tali categorie di dati ai soli incaricati espressamente autorizzati.	Art. 9 Reg. UE 2016/679	☑
Il Titolare ha provveduto ad adeguare le proprie informative al trattamento dei dati ed a fornire agli autorizzati le istruzioni in merito al rilascio dell'informativa ed all'eventuale acquisizione del consenso degli interessati.	Artt. 12,13,14 Reg. UE 2016/679	☑

www.incico.com

Il Titolare ha provveduto all'elaborare una procedura di riscontro delle istanze degli interessati allo scopo di consentire l'esercizio dei diritti agli stessi riconosciuti.	Artt. 15-21 Reg. UE 2016/679	☑
Il Titolare ha adottato una politica in materia di protezione dei dati personali e di sicurezza dei sistemi informativi, condivisa con tutte le funzioni aziendali (V. Manuale delle Contromisure).	Art. 24,25 Reg. UE 2016/679	☑
Il Titolare ha provveduto ad individuare i soggetti terzi che eseguono operazioni di trattamento per conto di INCICO S.P.A. ed a contrattualizzare i relativi rapporti.	Art. 28 Reg. UE 2016/679	☑
Il Titolare ha stabilito un piano formativo dei soggetti preposti al trattamento dei dati ed ha fornito brevi istruzioni operative in materia di trattamento dei dati.	Art. 29 Reg. UE 2016/679	☑
Il Titolare ha provveduto a redigere i Registri delle Attività di Trattamento del Titolare e del Responsabile allo scopo di acquisire contezza dei trattamenti posti in essere all'interno dell'azienda.	Art. 30 Reg. UE 2016/679	☑
Il Titolare ha eseguito una analisi e valutazione dei rischi incombenti sui dati (V. All.to A) ed ha verificato l'efficacia delle misure di sicurezza adottate.	Art. 32 Reg. UE 2016/679	☑
Il Titolare ha provveduto all'elaborare una procedura di data breach allo scopo di garantire la tempestiva notifica all'Autorità Garante per la Protezione dei dati Personali/comunicazione ai soggetti interessati qualora si verifichi una violazione di dati "rilevante".	Art. 32 Reg. UE 2016/679	☑
Il Titolare ha provveduto alla nomina volontaria di un proprio Data Protection Officer.	Art. 37 Reg. UE 2016/679	☑

Gli **impianti, i sistemi e le procedure di cui è dotata l'organizzazione appaiono soddisfacenti** al fine di garantire le opportune misure di sicurezza per il trattamento di dati personali dalla stessa eseguiti. Nel corso dell'anno 2023 sono quindi previsti unicamente interventi di manutenzione ordinaria.

Con cadenza annuale, il Titolare provvede ad eseguire una valutazione dei "Rischi Privacy" presenti/futuri allo scopo di implementare il proprio sistema di data protection, in relazione allo sviluppo tecnologico.

www.incico.com

8. Misure di sicurezza

Il Titolare, conformemente a quanto previsto dall'art. 32 Reg. UE 2016/679, ha:

□ adottato misure di sicurezza, fisica ed ambientale, adeguate allo scopo di minimizzare il rischio di accesso non consentito ai locali ove si svolge il trattamento;

□ disciplinato compiutamente il controllo degli accessi ai sistemi informativi contenenti dati personali allo scopo di minimizzare il rischio di accesso abusivo a sistema informatico, perdita, furto dei dati trattati attraverso strumenti informatici (Manuale delle Contromisure cui si rinvia);

□ definito un sistema di autenticazione informatica, allo scopo di attribuire a ciascun autorizzato proprie e riservate credenziali di accesso alle banche dati contenenti dati personali;

□ definito un sistema di ripartizione degli accessi, allo scopo di circoscrivere la sfera del trattamento consentito a ciascun autorizzato, in funzione delle mansioni svolte;

□ definito una politica di accesso alle reti ed ai servizi di rete.

Le misure di sicurezza adottate dal Titolare risultano disciplinate specificatamente nel Manuale delle Contromisure.

9. Procedura di Data Breach

Al fine di adempiere compiutamente agli obblighi posti a carico del Titolare del Trattamento ai sensi e per gli effetti degli agli artt. 33 e 34 Reg.UE 2016/679, INCICO S.P.A. ha elaborato la presente procedura volta a disciplinare le azioni da porre in essere qualora si verifichi una violazione di dati, cd. Data Breach.

9.1. Violazione di dati

Per data breach si intende un "incidente di sicurezza" che comporta, accidentalmente od illecitamente, la perdita dell'integrità, la cancellazione, la sottrazione, l'accesso o la divulgazione non autorizzata dei dati personali trattati dal Titolare.

Cause data breach	Eventi potrebbero comportare rischi per i diritti e le libertà degli interessati
Errore umano, condotta intenzionale illecita, reati informatici, eventi atmosferici avversi, cause di forza maggiore, mancato funzionamento delle misure di sicurezza adottate dal Titolare	Danni fisici, materiali o immateriali alle persone fisiche, perdita del controllo dei dati degli interessati, limitazioni dei diritti/discriminazione, furto o usurpazione di identità, perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Titolare), perdita di riservatezza dei dati personali protetti da segreto professionale (dati sanitari, giudiziari)

Ai sensi e per gli effetti degli artt.33 ss Reg. UE 2016/679, qualora si verifichi una violazione di dati incombe sul Titolare del Trattamento l'obbligo di:

- notificare l'accertata violazione all'Autorità Garante per la Protezione dei dati personali, salvo che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche;

- comunicare l'avvenuta violazione agli interessati, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati medesimi.

Tali comunicazioni sono funzionali ad attenuare i danni conseguenti alla violazione, aspetto particolarmente rilevante anche in relazione alle eventuali richieste risarcitorie, a consentire l'intervento delle pubbliche autorità, ove necessario, nonché a permettere ai soggetti interessati che subiscono la violazione di adottare le opportune cautele.

www.incico.com

9.2. Team di crisi

Il team di crisi di INCICO S.P.A. è composto da:

- Data Protection Officer (responsabile del Team)

- Amministratore di Sistema

Il Team di crisi può essere integrato dalle altre funzioni aziendali, di volta in volta coinvolte, in base alla tipologia di violazione (es. Contitolari, Responsabili del Trattamento).

Il Titolare, con il supporto del Data Protection Officer, ha il compito di provvedere, alla notifica/comunicazione dell'accertata violazione dei dati personali, come risulta dal Modello Organizzativo Privacy di INCICO S.P.A. nonché dalla nomina del RPD.

Con cadenza annuale, il RPD verifica la necessità/opportunità di apportare modifiche alla presente procedura in ragione degli eventi eventualmente verificatisi nel corso dell'anno.

9.3. Segnalazione

La segnalazione dell'incidente di sicurezza può provenire:

- Dall'interno dell'organizzazione

Al fine di garantire il tempestivo adempimento degli obblighi di cui agli arttt. 33 e 34 Reg.UE 2016/679, il Titolare ha provveduto ad istruire gli autorizzati in merito all'obbligo di comunicazione, a mezzo email, al Titolare medesimo o al RPD dell'avvenuta conoscenza di violazioni di dati personali, allo scopo di consentire l'immediata attivazione della procedura di valutazione dell'evento.

- Dall'esterno dell'Organizzazione

L'RPD raccoglie le segnalazioni di Data Breach provenienti dai Responsabile del Trattamento, eventuali sub-responsabili o contitolari, attraverso i canali definiti nei rispettivi accordi negoziali.

L'RPD trasmette, senza ingiustificato ritardo ed a mezzo mail, la ricevuta segnalazione, agli altri componenti del Team.

9.4. Valutazione di pertinenza della segnalazione

Raccolta la segnalazione, l'RPD informa tempestivamente l'altro membro del Team nonché altre eventuali funzioni aziendali potenzialmente coinvolte, sulla base delle informazioni disponibili.

Il Team, se necessario, procede alla raccolta di eventuali ulteriori informazioni allo scopo di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato. Qualora il Team ritenga che l'incidente di sicurezza non comporti un rischio per i diritti e le libertà degli interessati redige apposito verbale, trasmesso al Titolare, indicando le motivazioni poste alla base della valutazione ed aggiorna il Registro delle violazioni.

Qualora viceversa il Team ritenga che sussista un pericolo per i diritti e le libertà degli interessati, procede a:

1. informare per iscritto il Titolare del trattamento;

2. valutare le conseguenze dell'evento (dati personali colpiti, portata (n. e/o % interessati e n. dati), arco temporale, dati/interessati coinvolti);

Sulla base degli elementi raccolti, il team di crisi valuta la presenza o meno della violazione o presunta tale, tenendo presente che il Team, in caso di dubbio deve assumere un atteggiamento prudenziale a difesa dei diritti dell'interessato. In caso di esito positivo il team di crisi procede con l'analisi e la valutazione del rischio.

www.incico.com

L'esito della valutazione di pertinenza della segnalazione, anche qualora la stessa non risulti rilevante ai fini degli obblighi di cui agi artt.33 ss Reg.UE 2016/679 deve essere riportato, a cura del RPD, nel Registro delle Violazioni.

9.5. Identificazione di un potenziale data breach, analisi e valutazione del "rischio per i diritti e le libertà degli interessati"

Gli obblighi di notificazione e comunicazione di cui ai punti che precedono, sono strettamente legati al grado di rischio che la violazione potrebbe comportare per gli interessati.

In tal senso, l'obbligatorietà della notifica all'Autorità di Controllo è subordinata alla valutazione circa la probabilità che dalla violazione derivi un rischio per i diritti individuali e le libertà degli interessati, viceversa, l'obbligatorietà della comunicazione ai soggetti interessati è subordinata alla valutazione circa la probabilità che dalla violazione derivi un rischio elevato per i diritti degli interessati.

Le valutazioni in merito alla sussistenza ed al grado di probabilità del rischio spettano al Titolare.

Allo scopo di delimitare il "rischio" che una violazione dei dati personali può comportare occorre valutare se, ed in che termini, la violazione provochi o possa provocare:

"danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata". (Considerando n. 85 Reg.UE 2016/679).

Il Team di crisi procede all'analisi del rischio ed alla sua documentazione tenendo conto delle conseguenze dell'accertata violazione in termini di:

1. Riservatezza: stima del danno/impatto che la perdita di riservatezza riguardante l'asset comporterebbe per il business di INCICO S.P.A. /tutela degli interessati.

Rischio	Organizzazione	Interessati
Basso	I dati non presentano particolari requisiti di riservatezza per il Titolare	La perdita di riservatezza non ha impatti sui diritti degli interessati.
Medio	I dati risultano riservati per ragioni di business (concorrenza sleale, danno all'immagine), tuttavia un'eventuale diffusione non comporta elevati impatti sul business, sull'immagine aziendale, né determina inadempimento contrattuale, violazione di norme di legge.	La perdita di riservatezza ha impatti lievi sui diritti degli interessati.
Alto	I dati risultano riservati per ragioni di business (concorrenza sleale, danno all'immagine), un'eventuale diffusione comporta elevati impatti sul business e/o sull'immagine aziendale e/o, determina inadempimento contrattuale (NDA), e/o violazione di norme di legge.	La perdita di riservatezza ha un impatto elevato sui diritti degli interessati in termini di limitazione di diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita della sicurezza dei dati protetti da segreto professionale.

2. Integrità: stima del danno/impatto che la perdita di integrità riguardante l'asset comporterebbe per il business di INCICO S.P.A./tutela degli interessati.

Rischio	Organizzazione	Interessati
Basso	I dati non sono oggetto di transazioni economiche/finanziarie e non presentano particolari	La perdita di integrità non ha impatti sui diritti degli interessati.

www.incico.com

	requisiti di integrità. La perdita di integrità dei dati non comporta impatti sulle attività operative né sul rispetto della normativa vigente.	
Medio	La perdita di integrità dei dati non comporta elevati impatti sul business, sull'immagine aziendale, né determina inadempimento contrattuale e/o violazione di norme di legge.	La perdita di integrità ha impatti lievi sui diritti degli interessati degli interessati.
Alto	La perdita di integrità dei dati comporta elevati impatti sul business e/o sull'immagine aziendale e/o determina inadempimento contrattuale, e/o violazione di norme di legge.	La perdita di integrità ha un impatto elevato sui diritti degli interessati in termini di limitazione di diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita della sicurezza dei dati protetti da segreto professionale.

3. Disponibilità: stima del danno/impatto che la perdita di disponibilità riguardante l'asset comporterebbe per il business di INCICO S.P.A./tutela degli interessati.

Rischio	Organizzazione	Interessati
Basso	L'indisponibilità dei dati non determina inadempimenti contrattuali, commissione di reati o illeciti amministrativi.	La perdita di disponibilità non ha impatti sui diritti degli interessati.
Medio	L'indisponibilità dei dati determina inadempimenti contrattuali ma non responsabilità penali e/o illeciti amministrativi.	La perdita di disponibilità ha impatti lievi sui diritti degli interessati degli interessati.
Alto	L'indisponibilità dei dati determina inadempimenti contrattuali e/o commissione di reati e/o illeciti amministrativi.	La perdita di disponibilità ha un impatto elevato sui diritti degli interessati in termini di limitazione di diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita della sicurezza dei dati protetti da segreto professionale.

A seguito dell'analisi e valutazione del rischio, il Team di crisi, previa comunicazione scritta e confronto con il Titolare, individua le azioni da porre in essere:

1. Notificare l'accertata violazione all'Autorità Garante per la Protezione dei dati personali, salvo che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche;

2. Comunicare l'avvenuta violazione agli interessati, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati medesimi;

3. Individuare azioni correttive volte a minimizzare gli impatti per gli interessati e ripristinare la situazione precedente all'evento.

9.6. Azioni a seguito delle decisioni

9.6.1 Notifica all'Autorità Garante per la Protezione dei dati personali e termini

La violazione di dati personali deve essere notificata all'Autorità Garante per la Protezione dei Dati Personali, senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui il Titolare ne è venuto a conoscenza. In caso di ritardo nella notifica, la stessa dovrà essere corredata da giustificati motivi del ritardo.

www.incico.com

La notifica della violazione all'Autorità Garante per la Protezione dei dati personali, eseguita dal Titolare tramite il modello (allegato D) dovrà necessariamente contenere:

a) la descrizione della natura della violazione dei dati personali e, ove possibile, le categorie ed il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;

b) il nome ed i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) la descrizione delle probabili conseguenze della violazione dei dati personali;

d) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento allo scopo di porre rimedio alla violazione dei dati personali ovvero di attenuarne i possibili effetti pregiudizievoli;

Qualora e nella misura in cui non sia possibile fornire le predette informazioni contestualmente alla notifica, le stesse dovranno essere fornite, senza ulteriore ingiustificato ritardo, in fasi successive, includendo i motivi per cui non è stato possibile la comunicazione tempestiva.

9.6.2 Comunicazione agli interessati

Nei casi in cui il Team di crisi ritenga che la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare ha l'obbligo di comunicare la violazione all'interessato, senza ingiustificato ritardo.

La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali, deve indicare le informazioni e le misure di cui ai precedenti p.ti **b), c) e d)** e formulare, ove possibile, raccomandazioni per l'interessato intese ad attenuare i potenziali effetti negativi del data breach.

Si precisa come non sia richiesta la comunicazione all'interessato qualora:

- il Titolare abbia adottato adeguate misure tecniche ed organizzative di protezione (in particolare le misure destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura) e, le citate misure, risultino applicate ai dati personali oggetto della violazione;
- il Titolare abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Nei casi in cui la comunicazione del data breach agli interessati richiederebbe sforzi sproporzionati, il Titolare potrà procede ad una comunicazione pubblica o ad una misura simile, che consenta di informare gli interessati con analoga efficacia.

9.6.3 Azioni correttive

Il Team di crisi, laddove risulti possibile, individua e pone in essere una o più azioni volte a minimizzare gli impatti per gli interessati e ripristinare la situazione precedente all'evento, definendo modalità, responsabilità e tempi. Il team di crisi monitora lo stato di avanzamento delle azioni di trattamento e l'efficacia delle stesse, documenta l'attività compiuta e valuta la necessità di aggiornare l'analisi dei rischi, la P.I.A. se prevista per tale trattamento nonché, ove ritenuto necessario, altra documentazione (es. nomina a responsabile del trattamento).

9.7. Posizione del Titolare del Trattamento

Il Titolare del trattamento è tenuto informato degli sviluppi e delle decisioni del Team in ogni fase dell'indagine ed ha potere di imporre misure più restrittive a tutela dei diritti degli interessati.

Qualora Il Titolare non condividesse la decisione di procedere alla notifica/comunicazione adottata dal Team poiché ritenuta eccessiva in termini di impatto sulla reputazione/immagine della società, il Titolare medesimo si assumerà la responsabilità di imporre la propria decisione. In tali ipotesi, il Team crisi verbalizzerà la decisione del Titolare ed archivierà la documentazione senza procedere ulteriormente, dandone comunicazione avente data

www.incico.com

certa al Titolare.

9.8. Individuazione dell'Autorità di Controllo in caso di trattamento di dati personali transfrontaliero

Qualora una violazione dei dati personali coinvolga soggetti interessati in più di uno Stato Membro, il Titolare del Trattamento ha l'obbligo di notificare la violazione all'autorità di controllo capofila, che può essere identificata, ai sensi degli artt. 55 e 56 del GDPR, nell'autorità di controllo dello stabilimento principale - o dello stabilimento unico - del Titolare (o del responsabile del trattamento). In caso di dubbi circa l'identità dell'autorità capofila, il Titolare, potrà notificare la violazione all'autorità di controllo del luogo in cui si è verificata la violazione, precisando se la violazione possa aver coinvolto stabilimenti situati in altri Stati Membri e quali interessati, di altri Stati Membri, potrebbero essere stati coinvolti dalla violazione.

9.9. Registro delle violazioni

Ogni qualvolta sia accertata una violazione dei dati, seppur non sussistano gli obblighi di notifica all'Autorità di controllo e comunicazione agli interessati, il RPD, è tenuto ad aggiornare il Registro delle violazioni, allegato al Modello Organizzativo Privacy.

Nel Registro devono essere annotate, per ogni evento di *data breach*:

- le circostanze della violazione
- le conseguenze della violazione
- i provvedimenti adottati dal Titolare

Si precisa che, in caso di accertamento da parte del Garante, il Titolare sarà tenuto a fornire la documentazione relativa alle eventuali violazioni, ossia il Registro delle violazioni.

10. Procedura di riscontro delle istanze dell'interessato

Premesso che agli interessati è riconosciuto il diritto di chiedere contezza del trattamento eseguito su propri dati personali, da parte del Titolare, conformemente a quanto previsto dagli artt. 12 ss Reg.UE 2016/679, INCICO S.P.A. ha elaborato una procedura di riscontro delle istanze avanzate dagli interessati, allo scopo di individuare il soggetto preposto al riscontro delle richieste, le condizioni di legittimità delle richieste medesime nonché le modalità ed i termini di risposta/diniego.

10.1 Soggetto preposto al riscontro delle istanze dell'interessato

Il Titolare ha affidato al RPD il compito di riscontrare, per iscritto, le istanze formulate dall'interessato. A tal fine, i contatti del RPD risultano indicati nelle informative al trattamento dei dati predisposte dal Titolare.

E' compito del RPD annotare nel registro dei riscontri delle istanze degli interessati la data di ricevimento dell'istanza, il nominativo dell'interessato, la tipologia di richiesta e la data di riscontro.

10.2. Modalità ed oggetto della richiesta di informazioni

L'interessato deve inoltrare la propria istanza attraverso il canale di contatto indicato nell'informativa al trattamento dei dati personali. Ai sensi degli artt. 15 ss. Del Reg. UE 2016/679 l'Interessato può esercitare i seguenti diritti, alle condizioni di seguito indicate:

Diritto di accesso (Art. 15 Reg.UE 2016/679)	L'interessato ha diritto di richiedere conferma o meno che sia in corso un trattamento di propri dati personali e di ricevere informazioni relative all'origine dei dati, alle finalità, alle modalità ed alla durata del trattamento, ai soggetti terzi ai quali i dati vengono trasmessi, all'eventuale esistenza di un processo decisionale automatizzato. Qualora i dati siano trasmessi in paesi terzi (Extra UE) l'interessato ha diritto di essere informato dell'esistenza di garanzie adeguate.

www.incico.com

Diritto di rettifica (Art. 16 Reg.UE 2016/679)	L'interessato ha diritto di richiedere la rettifica dei propri dati qualora gli stessi risultino inesatti o l'integrazione dei propri dati qualora gli stessi risultino incompleti.
Diritto di cancellazione (diritto all'oblio) (Art. 17 Reg.UE 2016/679)	L'interessato ha diritto di richiedere la cancellazione dei propri dati qualora: a) i dati non siano più necessari rispetto alle finalità per i quali sono stati raccolti; b) l'interessato abbia revocato il proprio consenso al trattamento dei dati (nel caso in cui il trattamento sia basato sul consenso); c) l'interessato si opponga al trattamento e non sussista alcun motivo legittimo prevalente per procedere al trattamento oppure si oppone al trattamento per finalità di marketing diretto; d) i dati siano trattati illecitamente; d) la cancellazione dei dati sia imposta da un obbligo legale; d) il trattamento è relativo a dati personali, nell'ambito dell'offerta di servizi della società dell'informazione, siano relativi ad un minore di anni 16 e non sia stato autorizzato dal titolare della responsabilità genitoriale.
Diritto di limitazione del trattamento (Art. 18 Reg.UE 2016/679)	L'interessato ha diritto di richiedere la limitazione del trattamento qualora: a) contesti l'esattezza dei propri dati, in tale caso il Titolare dovrà limitare il trattamento per il periodo necessario a valutare la fondatezza delle contestazioni mosse dall'interessato; b) i dati siano trattati illecitamente e l'interessato si oppone alla cancellazione chiedendo, viceversa, che ne sia limitato l'utilizzo; c) benché il Titolare non abbia più necessità dei dati ai fini del trattamento, i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ed è in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare.
Diritto alla portabilità dei dati (Art. 20 Reg.UE 2016/679)	L'interessato ha diritto a ricevere i propri dati, in un formato strutturato di uso comune e leggibile da dispositivo automatico, ed ha diritto di richiedere la trasmissione di tali dati ad altro Titolare. Si precisa come il diritto in esame sia esercitabile unicamente nel caso in cui il trattamento sia basato sul consenso dell'interessato o sull'esecuzione di un contratto di cui lo stesso è parte contraente ed il trattamento sia effettuato con mezzi automatizzati.
Diritto di opposizione (Art. 21 Reg.UE 2016/679)	Qualora i dati siano trattati ai sensi dell'art.6 comma 1 lett. e) ed f) Reg.UE 2016/679 l'interessato ha diritto ad opporsi al trattamento, in qualsiasi momento per motivi connessi alla propria situazione particolare. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione, nella misura in cui sia connessa a tale marketing diretto.

10.3 Verifica dell'identità dell'interessato

Il RPD prima di procedere al riscontro, può richiedere all'interessato di fornire prova della propria identità qualora nutra ragionevoli dubbi circa l'identità dell'Interessato.

10.4 Modalità e termini di riscontro

L'istanza dell'interessato deve essere riscontrata dal RPD, per iscritto, senza ingiustificato ritardo **entro e non oltre un mese** dal ricevimento della stessa, fornendo le informazioni richieste in un formato strutturato di uso comune, salvo diversa indicazione dell'interessato medesimo.

www.incico.com

Il termine indicato può essere prorogato di due mesi, se necessario, in ragione della complessità dell'istanza o dell'elevato numero delle richieste. In tale ultima ipotesi il RPD è tenuto a indicare, nel riscontro, le motivazioni che giustificano il mancato rispetto del termine di un mese.

10.5 Ipotesi di diniego

Il Titolare può rifiutare di soddisfare l'istanza qualora, non possa essere stabilita l'identità dell'interessato ovvero qualora:

▪ la richiesta risulti illegittima, ovvero non rientri tra i diritti esercitabili dall'interessato;

▪ la richiesta risulti manifestamente infondata o eccessiva, ovvero la stessa richiesta sia stata reiterata, più volte, a breve distanza di tempo. In tale ultimo caso, il responsabile può addebitare all'interessato un contributo spese ragionevole. Al di fuori di tale ipotesi il riscontro non può comportare oneri e spese a carico dell'interessato;

▪ dall'esercizio dei diritti dell'interessato possa derivare un pregiudizio agli interessi tutelati in base alle disposizioni in materia di antiriciclaggio ed in materia di sostegno alle vittime di richieste estorsive ovvero allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria.

10.6 Notifica ai Responsabili del Trattamento

Qualora il RPD dia seguito ad una istanza di rettifica, cancellazione dei dati o limitazione del trattamento, lo stesso è tenuto a comunicare l'avvenuta rettifica, cancellazione dei dati o limitazione del trattamento ai terzi Responsabili del Trattamento ai quali i dati sono stati trasmessi, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Qualora ricorra tale ultima ipotesi, il RPD è tenuto ad informare prontamente il Titolare delle motivazioni dell'omessa comunicazione ai Responsabili del Trattamento.

11. Controllo generale sullo stato di sicurezza e audit

Il Titolare provvederà ad aggiornare le misure di sicurezza adottate, valutando gli strumenti e le conoscenze resi disponibili dal progresso tecnico, allo scopo di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento illecito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Titolare ed i soggetti da questo appositamente incaricati procedono, con frequenza almeno annuale, anche attraverso controlli a campione, a verificare:

- la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali, osservando particolari cautele per i supporti contenenti dati particolari categorie di dati;
- la correttezza dei profili di autorizzazione e delle procedure di autenticazione;
- l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici;
- l'integrità dei dati e l'efficienza delle procedure di back up e disaster recovery;
- la sicurezza delle trasmissioni in rete e dei sistemi antintrusione;
- la corretta distruzione e smaltimento dei supporti contenenti dati personali;
- il livello di formazione degli autorizzati;

Periodicamente, con frequenza annuale, verrà effettuato un l'audit di sicurezza volto a verificare che le misure implementate, sia quelle tecnologiche che quelle organizzative, risultino efficaci.

www.incico.com