Allegato B

Premesse

Il Comitato europeo per la protezione dei dati nella "*Opinion 3/2010 on the principle of accountability*" ha chiarito che "il titolare del trattamento dei dati debba essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi e che debba dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy."

Diventa, pertanto, funzionale individuare un apposito regolamento-documento che contenga le misure e le istruzioni per rendere l'Ente conforme al Regolamento (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "GDPR", Regolamento Generale Protezione Dati).

Il "PIANO GDPR dell'IRSAP" costituisce il Regolamento da aggiornare (quando necessario) in cui sulla base delle analisi svolte si definiscono le misure organizzative di tipo tecnico-giuridico-finanziario nel breve, medio e lungo periodo.

Sommario

Art. 1 Definizioni

Ai fini del presente regolamento si intende per:

1) «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 a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
2) «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, come 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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
4) «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.
5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a 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;

6) «base dati» e/o «banca dati»: 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;
7) «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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) «autorizzato al trattamento» e/o «designato al trattamento»: è la persona fisica, dipendente del Titolare che effettua materialmente le operazioni di trattamento sui dati personali. Gli autorizzati possono essere organizzati con diversi livelli di delega;
9) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, esterno all'Ente, che tratta dati personali per conto del titolare del trattamento.
10) «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. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
11) «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;
12) «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, che i dati personali che lo riguardano siano oggetto di trattamento.

13) «violazione dei dati personali» e/o «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;

14) «dati biometrici»: si intendono 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;

15) «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;

16) «dati giudiziari»: sono quelli relativi a condanne penali e a reati o a connesse misure di sicurezza.

Art. 2 Oggetto

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo, relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati

Il presente Regolamento intende disciplinare e regolare le procedure del modello privacy anche con riferimento ai ruoli dirigenziali ed alla gestione dei procedimenti amministrativi.

Il presente Regolamento contiene altresì una serie di allegati (Annex) che forniscono indicazioni operative generali sull'organizzazione dell'Ente e sulle istruzioni ai dipendenti in materia di conformità al GDPR.

Art. 3 Programmazione

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR:

- liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità, disponibilità e riservatezza.

Il Titolare pertanto nell'organizzazione della propria struttura interna, nonché nel perseguimento dei propri fini pubblici istituzionali, mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio dell'Ente, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

Art. 4 Finalità del trattamento

I trattamenti sono compiuti dall'IRSAP per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; rientrano in questo ambito i trattamenti compiuti per:
   - l'esercizio delle funzioni amministrative che riguardano il territorio, precipuamente nei settori organici dei servizi alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
   - l'esercizio di ulteriori funzioni amministrative per servizi di competenza dell'IRSAP in base allo Statuto ed alla vigente legislazione.
   - La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   - l'adempimento di un obbligo legale al quale è soggetto l'IRSAP. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   - l'esecuzione di un contratto con soggetti interessati;

- per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 5 Ruoli ed organigramma funzionale

L'IRSAP è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee.

Il Titolare provvederà a:

a) designare i Delegati del trattamento nelle persone dei Dirigenti delle singole strutture in cui si articola l'organizzazione dell'Ente, che saranno preposti a coordinare la gestione del Sistema Privacy nelle articolazioni organizzative di loro competenza.
b) qualora necessario per il corretto trattamento dei dati personali può avvalersi anche di soggetti privati esterni;
c) monitorare l'attuazione e la conformità al GDPR secondo quanto stabilito dalla legge, dai provvedimenti del Garante Italiano e dal Comitato Europeo, nonché da quanto previsto nel presente Regolamento.

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata ad IRSAP da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 GDPR.

L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

Art. 6 Responsabili del trattamento

Il Titolare, anche a mezzo delle deleghe ai Dirigenti di Area e degli Uffici Periferici, può avvalersi per il trattamento di dati personali, anche di categorie particolari e/o giudiziari, di soggetti privati esterni in qualità di responsabili del trattamento.

Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR nonché quanto stabilito dalle apposite Linee guida pubblicate dal Comitato Europeo per la Protezione dei Dati Personali.

È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario.

Le operazioni di trattamento in capo al Responsabile (primario o subordinato) possono essere effettuate solo da addetti che operano sotto la diretta autorità del medesimo attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

Il Responsabile del trattamento garantisce che chiunque agisca sotto la propria autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare ed in particolare:

a) alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
c) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
d) alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
e) ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
f) ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 7 Delegati e Referenti Gestione Sistema Privacy (RGSP)

I Dirigenti delle Aree, delle U.O.B. e degli Uffici periferici in cui si articola l'organizzazione dell'Ente, sono nominati Delegati per la gestione ed il monitoraggio dell'applicazione del sistema privacy dell'ufficio di appartenenza.

Ai predetti fini provvederanno, informandone il DPO, a nominare:

- Il Referente Gestione Sistema Privacy (RSGP) quale soggetto materialmente preposto al funzionamento ed implementazione del Sistema Privacy dell'Area, dell'U.O.B. e dell'Ufficio Periferico di appartenenza
- i dipendenti quali autorizzati al trattamento fornendo le idonee istruzioni.

I Referenti (RSGP) sono altresì nominati Responsabili Unici di tutte le banche dati di dati personali esistenti nell'articolazione organizzativa di rispettiva competenza.

I Dirigenti saranno, in ogni caso responsabili del trattamento di tutte le banche dati di dati personali esistenti nell'articolazione organizzativa di rispettiva competenza

Il RGSP deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

I RSGP supportano le strutture di vertice e i settori competenti, per tutte le questioni attinenti al trattamento dei dati personali e rappresentano l'interlocutore operativo verso l'ufficio del DPO.

I RSGP svolgono attività informativa nei confronti dell'Ufficio del DPO, in modo che questi abbia tutti gli elementi e riscontri che – unitamente alle evidenze della documentazione richiesta dal GDPR – i trattamenti di dati personali svolti nell'ambito di ogni struttura dell'Ente siano effettuati in conformità alle prescrizioni del GDPR e alle istruzioni del Titolare.

Art. 8 Responsabile della protezione dati

Il Responsabile della protezione dei dati (in seguito indicato con "DPO" e/o "RPD") è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna

per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti e dei RSGP.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

L'IRSAP assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/RSGP che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Così come stabilito agli artt. 37, 38 e 39 del GDPR il DPO:

a) opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati;
b) non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare – Legale rappresentante o suo delegato -.

Art. 9 Formazione del personale

Il GDPR prevede l'obbligo della formazione per le pubbliche amministrazioni, in materia di protezione dei dati personali per tutte le figure presenti nell'organizzazione (sia dipendenti che collaboratori), anche quale misura di sicurezza.

La formazione deve presentare caratteristiche di interdisciplinarietà ed essere finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.

La formazione dovrà avvenire su più livelli:

1) Nella fase del percorso di adeguamento sarà opportuno programmare almeno una giornata formativa di base, aperta a tutti i dipendenti e sugli strumenti di attuazione da mettere in atto.
2) Nella fase successiva la formazione può svolgersi nell'ambito dell'applicazione operativa del sistema di gestione privacy e del presente Provvedimento.

Il DPO ha il compito di sorvegliare sulle attività di sensibilizzazione e formazione in relazione al trattamento dei dati personali dirette al personale interno.

Art. 10 Registri dei trattamenti

Il Registro Unico dei trattamenti ex art. 30 GDPR è messo a disposizione da parte del Titolare del trattamento su richiesta dell'Autorità di controllo.

Con apposito provvedimento interno il Titolare delegherà i Dirigenti ed i RSGP di appartenenza alla tenuta del Registro dei Trattamenti

Art. 11 Registro di accountability

Il Registro di accountability è necessario al fine di registrare e tenere traccia di tutte le attività che l'Ente svolge in materia di protezione dei dati personali.

Il Titolare conserverà e aggiornerà il Registro Generale di accountability riferito alla conformità dell'intero Ente,

Con apposito provvedimento interno il Titolare delegherà i Dirigenti ed i RSGP di appartenenza alla tenuta e all'aggiornamento del Registro di accountability

Art. 12 Valutazioni d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa.

Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica.

Il Titolare deve consulterà il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato.

Il Titolare può decidere di pubblicare sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 13 Violazione dei dati personali-Procedura

Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'IRSAP.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede ad attivare la seguente procedura:

A) La segnalazione viene inoltrata all'RGSP di competenza della struttura di appartenenza e viene immediatamente informato il DPO;

B) Si avviano gli accertamenti dovuti per comprendere il contesto del trattamento, la natura dei dati personali coinvolti e qualunque informazione utile per una completa valutazione dell'episodio;

C) Conclusi gli accertamenti e comunque non appena vengano individuati elementi chiari per la valutazione dell'episodio, si procederà a seconda dei casi a:

C.1) chiudere l'accertamento senza annotazione nel registro delle violazioni qualora sia esclusa in modo chiaro una violazione dei dati personali

C.2) annotare la violazione dei dati personali nel Registro, senza effettuare alcuna notificazione qualora vi sia un rischio improbabile per i diritti e le libertà degli interessati;

C.3) annotare la violazione dei dati personali nel Registro ed effettuare la notificazione al Titolare, all'Autorità di Controllo nonché la comunicazione agli interessati.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, valuterà se effettuare l'eventuale comunicazione all'Autorità Garante nonché le comunicazioni agli interessati.

Tale comunicazione, che sarà sottoscritta dal legale rappresentante del titolare del trattamento, deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 3 giorni; tale termine decorre dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza dal verificarsi della violazione.

Si specifica inoltre che nel caso in cui la comunicazione di cui al punto 3 sia effettuata successivamente al termine dei 3 giorni, questa deve essere corredata delle ragioni del ritardo. E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione, anche a seguito di ulteriori indagini e attività di follow-up (c.d. notificazione in fasi)

Il Dirigente della struttura organizzativa trattante il dato violato coordina e verifica lo svolgimento della procedura di documentazione nell'apposito registro dell'episodio di violazione e che venga riportata anche la scelta e le motivazioni relative alle decisioni sulla necessità di notificare o meno l'evento.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

Art. 14 Canali di comunicazione.

Al fine di creare un sistema di comunicazione tra dipendenti RSGP, DPO per quesiti, aggiornamenti ed indicazioni su casi concreti, viene istituita una email dpo@irsapsicilia.it che può essere utilizzata per richieste e comunicazioni al DPO.

Art. 15 Procedimento amministrativo e dati personali

Salvo diverse e più specifiche istruzioni e regolamenti interni il trattamento dei dati personali nell'ambito dei procedimenti amministrativi interni ed esterni deve tenere conto dei seguenti criteri:

a) formazione degli atti in originale in formato digitale (art. 40, Cad), la produzione degli atti in cartaceo o la formazione di un atto in formato analogico deve avvenire solo quando non è possibile la modalità ordinaria prevista dalla legge;
b) la costruzione dei contenuti di atti e provvedimenti recanti informazioni personali deve tener conto dei principi di necessarietà e pertinenza del dato personale riportato rispetto alla finalità giuridica del provvedimento in cui è riportato;
c) il soggetto (persona fisica e giuridica) indicato in atti e documenti è identificato esclusivamente con il codice fiscale e/o partita iva senza indicazioni ultronee di data e luogo di nascita o luogo di residenza, recapito, sede, etc.;
d) la tutela del dato va accompagnato da una continua analisi di sviluppo dell'attività istituzionale che deve tener conto dei principi di semplificazione documentale e snellimento procedimentale, nonché economicità degli atti prodotti;
e) al fine di agevolare l'individuazione del fascicolo l'oggetto di qualsiasi comunicazione (anche interna) o provvedimento deve indicare gli estremi del fascicolo istituito.

Art. 16 Amministrazione trasparente

Il Titolare provvederà, a conformarsi alle Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, pubblicate nel Registro dei provvedimenti del Garante Privacy al n. 243 del 15 maggio 2014 e pubblicate sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014.

In via generale si stabilisce che andranno distinte, considerato il profilo del diverso regime giuridico applicabile, le disposizioni che regolano gli obblighi di pubblicità dell'azione amministrativa per finalità di trasparenza da quelle che regolano forme di pubblicità per finalità diverse (es.: pubblicità legale).

Gli obblighi di pubblicazione online di dati per finalità di trasparenza sono quelli indicati nel d. lgs. n. 33/2013 e nella normativa vigente in materia avente ad oggetto le

informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.

Accanto ai suddetti obblighi di pubblicazione permangono altri obblighi di pubblicità online di dati, informazioni e documenti della P.A. contenuti nelle specifiche disposizioni di settore.

In tutti i casi, indipendentemente dalla finalità perseguita, laddove la pubblicazione online di dati, informazioni e documenti, comporti un trattamento di dati personali, devono essere opportunamente contemperate le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali, nonché la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Si stabilisce che il presente regolamento dovrà essere pubblicato nel sito web istituzionale dell'IRSAP, nella sezione "Atti generali" all'interno della sezione "Amministrazione trasparente".

Si provvederà ad attivare, all'interno della sezione "Amministrazione trasparente", anche un'apposita sezione "Privacy" all'interno della quale pubblicare la nomina del DPO ed ogni eventuale ulteriore pubblicazione, anche in conformità del presente Regolamento, che sia necessario rendere consultabile.

Art. 17 Misure di sicurezza

L'Ente adotterà misure di sicurezza organizzative, fisiche e logiche, adeguate alle operazioni di trattamento di dati personali effettuate.

La sicurezza del dominio dell'Ente non dipende solo da aspetti tecnici, ma anche da quelli organizzativi, sociali e legali e deve essere pertanto vista come caratteristica globale, in grado di fornire, anche in considerazione delle mutevoli necessità e tecnologie, il desiderato livello di tutela dei dati, in particolare quelli personali.

L'Ente fissa come obiettivo quello di realizzare un proprio sistema informativo sicuro tale che soddisfi le seguenti proprietà:

a) Disponibilità: le informazioni ed i servizi che eroga devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio.
b) Integrità: le informazioni ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione.
c) Confidenzialità o Riservatezza: le informazioni che contiene possono essere fruite solo dalle persone autorizzate a compiere tale operazione.

Ai predetti fini il sistema informatico dell'Ente, sia a livello centrale che periferico, verrà adeguato progressivamente alle misure di sicurezza adeguate prescritte dall'art. 32 GDPR, mediante la definizione dei profili di sicurezza ad efficacia crescente, da associare alle varie tipologie di trattamento, ponendo come profilo minimo le misure emanate da AGID con la Circolare n.2/2017 del 18 aprile 2017 "Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni".

Art. 18 Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti.

Annex 1 Schema generale dell'organigramma funzionale.

Organizzazione	Ruoli e responsabilità in relazione al GDPR ed ai relativi processi
Istituto Regionale per lo Sviluppo delle Attività Produttive (IRSAP)	**Ruolo GDPR:** Assume, a norma dell'Art. 4 punto 7 del GDPR, il ruolo di Titolare dei trattamenti afferenti alle finalità di cui all'Atto costitutivo e allo Statuto.
Il Legale Rappresentante	**Ruolo GDPR:** Assume la figura di Delegato del Titolare per i trattamenti di sua diretta responsabilità. Assolve, nelle forme più opportune, all'attuazione dell'organizzazione e dei processi in materia di data protection. **Processo Formazione degli atti** (data protection by design/default) Con il supporto del RPD, approva atti di organizzazione o di indirizzo al fine di garantire la compliance al GDPR Cura per mezzo dell'Ufficio della Direzione Generale la conservazione e aggiornamento del Registro Generale dei Trattamenti. **Processo Accountability** Adozione di atti di organizzazione idonei a garantire la compliance al GDPR sentito il RPD **Processo di gestione degli incidenti** Provvede a far attuare, su indicazione dell'ufficio del DPO, le misure organizzative o tecniche tese a diminuire i rischi e le probabilità di incidente nell'ambito dei trattamenti di sua responsabilità.
I Dirigenti – Delegati al trattamento	**Ruolo GDPR:** Assumono il ruolo di Delegati del Titolare per i trattamenti di loro diretta responsabilità ai sensi dell'art. 2-quaterdecies del Codice Privacy. **Processo di formazione degli atti:** Curano la gestione del Registro Dei Trattamenti per le attività di competenza. Predispongono gli atti, emettono indirizzi e istruzioni operativi per il personale in relazione e al rispetto del GDPR, con il supporto dei Referenti Interni Gestione Privacy e dell'ufficio del DPO

	Processo di Accountability Organizzazione della documentazione relativa ai trattamenti di cui sono titolari o responsabili. Monitorano l'adeguata conservazione e aggiornamento del Registro Accontability **Processo di gestione degli incidenti** Ricevono o rilevano incidenti che coinvolgono trattamenti di cui sono titolari, concorrono alla determinazione della gravità dell'incidente e determinano le comunicazioni da fare al garante, alla autorità giudiziaria, in collaborazione con il DPO. **Processo dei diritti degli interessati** Collaborano attivamente con il DPO e l'Ufficio del DPO al fine di rispondere nei tempi previsti alle richieste degli interessati, del garante o dell'autorità giudiziaria.
Referente Sistema Gestione Privacy	**Ruolo GDPR:** Assumono il ruolo di Autorizzati per i trattamenti di loro diretta responsabilità ai sensi dell'art. 2-quaterdecies del Codice Privacy. **Processo di formazione degli atti** Una o più figure che supportano l'attività implementazione e funzionamento del sistema privacy individuato in ogni struttura organizzativa dell'Ente e che assiste il Dirigente, di concerto con il DPO nella individuazione dei trattamenti, nella formulazione delle DPIA, nella predisposizione di atti e convenzioni che prefigurino dei rapporti inerenti la Data Protection.. **Processo di accountability** Supportano l'attività di consulenza ai settori nei processi di verifica e controllo, collaborando con il DPO. Curano la conservazione e aggiornamento del Registro Accontability **Processo di gestione degli incidenti** Ricevono gli avvisi di eventuali incidenti di sicurezza e ne riferiscono al Dirigente, al DPO ed al Titolare Attivano la procedura in caso di violazione di dati personali
Autorizzati al trattamento	**Ruolo GDPR:** Assumono il ruolo di Autorizzati per i trattamenti di loro diretta responsabilità ai

	sensi dell'art. 2-quaterdecies del Codice Privacy. **Processo di formazione degli atti:** Svolgono specifici compiti e funzioni connessi al trattamento di dati personali nell'ambito della propria attività lavorativa sulla base di opportune autorizzazioni ed istruzioni. **Processo di Accountability** Sono nominati dal Titolare, anche per mezzo dei Delegati e con il supporto del DPO in relazione alle istruzioni da fornire **Processo di gestione degli incidenti** Qualora hanno notizia di un incidente di sicurezza che comporta una violazione dei dati personali devono riferirne al RSGP **Processo dei diritti degli interessati** Collaborano attivamente con il DPO al fine di rispondere nei tempi previsti alle richieste degli interessati, del garante o dell'autorità giudiziaria.
Data Protection Officer	**Ruolo GDPR** vedi artt. 38 e 39 del GDPR **Processo di formazione degli atti**: Gestisce il registro dei trattamenti per quanto attiene il rispetto al GDPR; verifica e supporta il titolare e i suoi delegati nella tenuta del registro dei trattamenti e garantisce adeguata consulenza giuridica, tecnologica e organizzativa nella formulazione delle DPIA, se richiesto, e nella formulazione di atti convenzionali, contratti o protocolli di intesa. **Processo di Accountability** Svolge attività di verifica connesse all'attuazione del principio di accountability e si avvale delle strutture dell'ente ed in particolare del responsabile dei sistemi informativi **Processo di gestione degli incidenti** Rileva le segnalazioni degli incidenti e congiuntamente con il titolare del trattamento ne predispone la valutazione e persegue le azioni necessarie in modo diretto o dando indicazioni per il loro assolvimento. **Processo dei diritti degli interessati** In carico al DPO che si avvale della collaborazione delle strutture organizzative dell'Ente al fine del rispetto dei tempi

Annex 2 Compiti dei dirigenti e dei Responsabili Sistema Gestione Privacy

I Dirigenti:

a) al momento della predisposizione di atti amministrativi individuano se quell'atto prefigura o interviene in processi che prevedono il trattamento di dati personali, nonché se è necessario prevedere la stipula di appositi accordi e/o istruzioni di protezione dati in base alle regole dedicate ai rapporti con i terzi. In tale caso con il supporto del DPO e dei RGSP individuano i trattamenti e ne avviano la registrazione nell'apposito registro.

b) I Dirigenti potranno:

- richiedere pareri ai RSGP, e se ritenuto necessario, consultare il DPO per tutte le questioni riguardanti la individuazione dei trattamenti, delle loro caratteristiche e delle azioni da porre in essere per la loro corretta gestione nel tempo.
- coinvolgere i RSGP con il supporto dell'ufficio del DPO, ai fini della valutazione ed esecuzione della DPIA.

c) richiedono il parere del DPO a chiusura della DPIA.

d) in fase di monitoraggio da parte dell'ufficio del DPO, fornire la massima collaborazione tesa ad evidenziare problemi ed ad individuare soluzioni, in fase di segnalazioni da parte di interessati provvedere, con il supporto eventuale del DPO o del suo ufficio, a mettere in atto misure adeguate a rendere conto delle situazioni oggetto di segnalazione ed eventualmente a mettere in atto misure idonee alla risoluzione dei problemi evidenziati

e) in fase di ispezione o indagine del Garante offrire tutta la collaborazione possibile.

I Dirigenti, al momento della definizione del trattamento, identificano e mettono in atto le procedure idonee a fornire adeguata informativa agli interessati.

Per la corretta individuazione dei contenuti e della forma dell'informativa, essi si avvalgono dei fac simili messi a disposizione dall'ufficio del DPO.

I RSGP, coadiuvano e supportano i Dirigenti, in collaborazione con il DPO, le strutture di appartenenza, nei seguenti compiti e con le seguenti finalità:

a. l'aggiornamento della mappa dei processi;

b. la formazione degli atti al fine di garantire il principio di data protection by design (delibere, decreti, bandi gara, contratti, convenzioni, ecc.);
c. l'individuazione e la registrazione corretta dei trattamenti, a supporto dei dirigenti;
d. la predisposizione delle informative da dare agli interessati sulla base delle indicazioni del DPO;
e. in accordo con il DPO, l'individuazione e la valutazione dei rischi in fase preventiva e di DPIA;
f. la verifica che il personale sia informato e formato sui temi del GDPR e che gli autorizzati abbiano ricevuto e compreso le istruzioni, al fine di assicurare quanto previsto art. 39 lettera a) del GDPR e art. 2-quaterdecies decreto legislativo n. 196/2003;
g. la piena e fattiva collaborazione all'ufficio del DPO in caso di incidente/data breach e per tutte le azioni conseguenti, nonché in caso di ispezione o indagine delle Autorità di controllo.

Annex 3 Responsabili del trattamento

Il DPO fornirà un modello generale di accordo per la nomina a Responsabile del trattamento in conformità con l'art. 28 dek GDPR nonché delle Linee Guida pubblicate dal Comitato Europeo per la Protezione dei Dati Personali

All'interno del sistema informatico dell'IRSAP verrà creata una cartella denominata RESPONSABILE_DEL_TRATTAMENTO al seguente percorso informatico:

- \\ _____\…\Privacy\RESPONSABILE_DEL_TRATTAMENTO

All'interno della cartella si provvederà, previa comunicazione del Dirigente di riferimento (tramite email sistemagdpr@irsapsicilia.it), a creare un'ulteriore cartella per ogni responsabile. All'interno delle suddette cartelle verranno salvati i contratti/atti giuridici che disciplinano i rapporti tra titolare del trattamento e responsabile del trattamento.

L'accesso alla cartella condivisa è possibile per ogni Dirigente, per ogni referente designato, nonché per il DPO.

I file dovranno essere protetti, per la modifica, da password, quindi ogni modifica deve avvenire tramite il responsabile informativo dell'Ente.

I designati provvederanno a segnalare eventuali nomine, nonché i relativi contratti/atti.

Annex 4 Registro dei trattamenti

In merito al Registro Unico del trattamento sarà necessario procedere ad una approfondita e dettagliata analisi dei trattamenti collegati ai sistemi di flusso informativi dell'Ente sulla base degli elementi che seguono:

a. analisi delle funzioni delle strutture organizzative (direzioni, aree ed uffici) rapportato alle singole attività procedimentali e non;
b. tipologia delle attività in procedimentali e non procedimentali;
c. tipologia dell'attività inerente il trattamento (procedimento d'ufficio o su istanza, attività ordinaria corrente o attività sviluppata su evento non ordinario);
d. regime amministrativo applicato al trattamento o attività secondo le disposizioni della legge Madia (autorizzazione, concessione, scia, scia condizionata, attività libera);
e. termini procedimentali (qualora esistenti);
f. tipologia di dati trattati (anonimi, comuni, particolari – sensibili, giudiziari, salute, disagio economico-sociale);
g. ambito del trattamento (comunicazione o diffusione);
h. strutture organizzative interne coinvolte;
i. strutture o soggetti esterni coinvolti o destinatari di comunicazioni;
j. fasi del trattamento e delle attività comprensive delle fasi di identificazione con lo SPID (sistema pubblico di identità digitale) e le attività di pagamento digitale (PagoPA);
k. formato dei dati (carta, digitale, open);
l. piani di intervento per implementazione misure adeguate nel breve, medio e lungo periodo sulla base del rischio e delle possibilità finanziarie.

Nell Registro Unico dei trattamenti verranno annotati tutti i trattamenti di pertinenza che i Dirigenti, unitamente ai RGSP e di concerto con il DPO, riterranno indispensabile iscrivere

In particolare ogni Area, U.O.B e ogni Ufficio periferico dovrà provvedere periodicamente a:

a) Verificare la corrispondenza dei propri trattamenti con quelli iscritti nel registro.
b) Proporre al DPO di inserire nuovi trattamenti di dati personali all'interno del registro oppure di chiederne la modifica o cancellazione.

I trattamenti potranno essere o interni o esterni; in quest'ultimo caso dovrà essere trasmesso il contratto di servizio e la nomina del responsabile esterno secondo lo schema concordato con il DPO.

Il Registro Unico dei trattamenti sarà tenuto in formato elettronico e collocato nella cartella condivisa nel seguente percorso informatico:

- \\ _____\…\Privacy\REGISTRO_UNICO

L'accesso alla cartella condivisa è possibile per ogni Dirigente, per ogni RSGP, nonché per il DPO.

Il file deve essere protetto, per la modifica, da password, quindi ogni modifica deve avvenire tramite il Responsabile Informatico dell'Ente.

I designati provvederanno a segnalare eventuali aggiornamenti al Registro tramite mail sistemagdpr@irsapsicilia.it, da attivare..

Il registro di trattamento dovrà contenere almeno le seguenti informazioni:

a) il nome ed i dati di contatto dell'IRSAP, del Legale rappresentante e, se nominato, del suo Delegato, eventualmente del Contitolare del trattamento, del RPD;
b) il nome ed i dati di contatto dell'Area, dell'Ufficio Periferico dell'IRSAP, del Dirigente e del Responsabile Sistema di Gestione Privacy, del RPD
c) le finalità del trattamento;
d) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
f) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
g) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Unitamente al registro dei trattamenti, viene costituito il registro unico delle violazioni, che sarà tenuto nella medesima cartella del registro generale dei trattamenti sopra indicato e che seguirà il medesimo iter funzionale del registro dei trattamenti

Annex 5 Processo accountability

Per un'efficace applicazione del GDPR e del rispetto del principio di accountability, in particolare, è opportuno che il sistema organizzativo includa la rilevazione dei processi che evidenzi il complesso delle attività svolte, la loro sequenza e le modalità con cui sono corrispondentemente effettuate.

Il principio di accountability sancito dal regolamento europeo in materia di protezione dei dati richiede che l'organizzazione e i processi, siano impostati in modo tale a rendere possibile la attività di "rendere conto" delle misure messe in atto per la protezione dei dati.

L'organizzazione dell'ente può essere chiamata a rendere conto in varie circostanze:

a) su istanza del Garante in attività ispettiva o a seguito di segnalazioni o denunce

b) su istanza degli interessati nell'esercizio dei loro diritti

c) su istanza del DPO in attività di monitoraggio o a seguito di segnalazioni da parte degli interessati.

Il Registro di accountability dovrà registrare quanto mento i seguenti dati:

1) Nome del RGSP;
2) Data della registrazione;
3) Evento registrato con oggetto le attività svolte per la gestione del sistema protezione dati personali e che a titolo esemplificativo e non esaustivo possono riguardare:
   - Formazione dei dipendenti;
   - Svolgimento DPIA;
   - Modifiche e/o integrazioni al registro dei trattamenti;
   - Cambiamenti (anche negativi) e/o aggiornamenti al sistema di conservazione documentale cartaceo e/o informatico;
   - Cambiamenti (anche negativi) e/o aggiornamenti al sistema informatico;
   - Cambiamenti (anche negativi) e/o aggiornamenti delle misure di sicurezza fisiche e/o logiche;
   - Registrazioni nel registro delle violazioni;
   - Consultazioni, pareri del DPO.
4) Conseguenze e/o effetti dell'evento;
5) Note (eventuali).

Viene costituito il registro unico di acoountability dell'Ente, le cui modalità di gestione sono identiche a quelle previste per il registro generale dei trattamenti

Sarà creata, anche in questo caso, una cartella condivisa denominata REGISTRO_DELLE_ATTIVITA al seguente percorso informatico:

- \\ _____\…\Privacy\REGISTRO_DELLE_ATTIVITA;

L'accesso alla cartella condivisa è possibile per ogni Dirigente, per ogni referente designato, nonché per il DPO.

Il file deve essere protetto, per la modifica, da password, quindi ogni modifica deve avvenire tramite il Responsabile Informatico dell'Ente..

I designati provvederanno a segnalare eventuali aggiornamenti al Registro delle attività tramite mail sistemagdpr@irsapsicilia.it, da attivare,

-

Annex 6 Valutazione di Impatto DPIA

L'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, come individuati dalle Linee guida sulla valutazione dell'impatto sulla protezione dei dati (DPIA) (wp248rev.01) ai sensi degli artt. 35, par. 4, e 57, par. 1, lett. k), del GDPR1 sono:

- In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);

1) - trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).
2) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
3) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

4) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
5) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;
6) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
7) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
8) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
9) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
10) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.
11) Nel caso in cui un trattamento soddisfi almeno quattro dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA.

Il RPD monitora lo svolgimento della DPIA.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati.

   Sono altresì indicati:

   - i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;

- una descrizione funzionale del trattamento;
- gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
- valutazione della necessità e proporzionalità dei trattamenti, sulla base:
  - delle finalità specifiche, esplicite e legittime;
  - della liceità del trattamento;
  - dei dati adeguati, pertinenti e limitati a quanto necessario;
  - del periodo limitato di conservazione;
  - delle informazioni fornite agli interessati;
  - del diritto di accesso e portabilità dei dati;
  - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
  - dei rapporti con i responsabili del trattamento;
  - delle garanzie per i trasferimenti internazionali di dati;
  - consultazione preventiva del Garante privacy;

b) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

c) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati.

La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Annex 7 Misure di Sicurezza

In linea generale le attività di sviluppo di un sistema di sicurezza sono generalmente raggruppabili all'interno delle seguenti aree:

a) Sicurezza Fisica;

Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo. I requisiti di sicurezza fisica possono variare considerevolmente in funzione delle dimensioni e dell'organizzazione del sistema informativo. L'attivazione misure di sicurezza fisica (porte, sistema antincendio, antifurto etc.), funzionali al sistema informatico o di archiviazione cartacea spettano alla struttura competente in materia di manutenzioni e lavori pubblici. Le contromisure di sicurezza fisica possono essere ricondotte alle seguenti:

- Sicurezza di area. - La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono ai controlli fisici all'accesso, alla sicurezza dei computer e dei server rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.
- Sicurezza delle apparecchiature hardware. - La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissione o furti.

b) Sicurezza Logica:

La sicurezza logica è una componente particolarmente critica della sicurezza del sistema informativo. Il campo di applicazione della sicurezza logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le misure di sicurezza logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico (Information and Communication Technology) e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

c) Sicurezza Organizzativa.

Il processo della sicurezza dei sistemi informativi automatizzati richiede che, accanto all'adozione di misure tecnologiche, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo medesimo. Gli aspetti organizzativi della sicurezza dei sistemi informativi automatizzati riguardano principalmente:

- la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate. In relazione al primo aspetto, con riferimento alle funzioni organizzative dovranno essere identificati una serie di ruoli, compiti e responsabilità per le specifiche attività del processo della Sicurezza.

Il Monitoraggio tecnologico è in carico alla Direzione e al Responsabile informatico dell'Ente che provvede:

a) alla redazione e attuazione di un piano per le verifiche sulle misure di sicurezza messe in atto dai dirigenti responsabili dei sistemi e delle applicazioni o di fornitori esterni;
b) alla verifica della rispondenza delle misure di sicurezza in essere alle linee guida emesse dal DPO;
c) alla relazione periodica sulle misure di sicurezza adottate evidenziando punti di criticità e proponendo remediation plan.

I dirigenti responsabili per ambiti di competenza debbono assicurare:

a) tutte le condizioni idonee di collaborazione alla Direzione e al Responsabile Informatico al fine di consentire un efficiente ed agevole lavoro dell'Ufficio;
b) l'attuazione del piano indicato dalla Direzione nei tempi indicati dallo stesso;
c) fornire il supporto in caso di segnalazioni di incidenti al fine di comprendere la gravità degli stessi;
d) la tempestiva segnalazione al Responsabile Informatico della evidenza di incidenti che possono aver coinvolto dati personali.

Annex 8 Amministrazione trasparente

I soggetti pubblici possono diffondere dati personali solo se ciò è ammesso da una specifica disposizione di legge, in assenza di una disposizione di legge o, nei casi previsti dalla legge, di regolamento, nonché, ferma restando la tutela della privacy, per rispondere al principio generale della trasparenza della P.A e della tutela del diritto di accesso generalizzato dell'utenza civile.

Prima di pubblicare sui siti web istituzionali informazioni, atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, il Dirigente responsabile della sua pubblicazione deve selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni.

Il Dirigente è tenuto a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità, fatte salve le esigenze di trasparenza dell'Ente.

Nel caso di provvedimenti che riconducano a rapporti giuridici con l'Ente (incarichi, appalti, convenzioni etc), il dirigente dovrà accertarsi che, oltre ai dati anagrafici, le pubblicazioni non contengano altri elementi identificativi quali abitazione privata, numero di telefono, email, etc.

Anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d.lgs. n. 33/2013, non è possibile comunque «rendere […] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione».

I dati personali che risultano non adeguati, non pertinenti e non limitati a quanto necessario rispetto alle finalità di trasparenza non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online.

In caso contrario, occorre provvedere al relativo oscuramento.

Il procedimento di selezione dei dati personali che possono essere pubblicati online deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni sono idonee a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, «particolari categorie di dati», oppure nel caso di «dati relativi a condanne penali o reati»

Effettuata la previa valutazione circa i presupposti e l'indispensabilità della pubblicazione di dati sensibili e giudiziari, devono essere adottate idonee misure e accorgimenti tecnici volti a evitare «la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo»

In tali casi e per tali tipologie di dati sensibili, per la pubblicazione dei relativi documenti, occorrerà procedere alla indicazione in forma anonima dei dati personali (art. 7-bis, comma 3, del d. lgs. n. 33/2013).

Non è mai ammessa la pubblicazione di dati relativi a stati di salute, e i relativi provvedimenti dovranno prevedere l'oscuramento dei dati anagrafici e di tutti i dati che possono ricondurre all'individuazione del soggetto oggetto del trattamento.

Allegati

All.1: Procedura data breach IRSAP

All.2: Scenari data breach

All.3: Modello registro trattamenti.

All.4: Modello registro violazioni.

All.5: Modello registro accountability

All.6: Modello comunicazione all'interessato.

All.7: Modello scheda violazione informazioni.

All.8: Direttiva cloud.

All.9: Modello scheda censimento azienda.

All.10: Informativa completa censimento imprese.

All 11: Informativa semplificata censimento imprese.

All.12: Informativa trattamento dati personali web.

All.13: Informativa semplificata COVID

All.14: Informativa semplificata dipendenti.

All.15: informativa professionisti, consulenti, collaboratori esterni

ALLEGATO B

ALLEGATI AL REGOLAMENTO

PROCEDURA "DATA BREACH"

REGOLAMENTO UE 679/2016

SOMMARIO

1. SCOPO

Scopo della procedura è definire le modalità e le responsabilità in caso di violazione dei dati personali al fine di garantire:

a) l'identificazione della violazione;
b) l'analisi delle cause della violazione;
c) la registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse;
d) la definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;

nonché, ove necessario

e) la notifica di una violazione dei dati personali all'autorità di controllo;
f) la notifica di una violazione dei dati personali agli interessati.

2. CAMPO DI APPLICAZIONE

La procedura è applicabile a tutte le attività svolte da IRSAP, (di seguito anche soltanto "Titolare"), con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (dipendenti, cittadini, altri soggetti terzi), anche con il supporto di fornitori esterni.

3. DEFINIZIONI E ABBREVIAZIONI

3.1. Definizioni

Pur rinviando per l'elenco completo delle definizioni all'Art. 4 del REGOLAMENTO (UE) 2016/679, qui di seguito si riporta che:

1) **«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 a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) **«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, come 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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) **«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;
4) **«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici

applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

5) **«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;
6) **«violazione dei dati personali»**: 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.

3.2. Abbreviazioni

- **RPD**: Responsabile per la protezione dei dati personali;
- **RTDP**: Responsabile della tutela dei dati personali e della sicurezza dei dati aziendali;
- **RAD**: Responsabile Area Dirigenziale.

4. RESPONSABILITÀ

- **RAD** Segnalazione al RTDP ed al RPD delle violazioni, rilevate e/o che gli sono state segnalate dai dipendenti della propria Area, su dati personali digitalizzati e/o archiviati analogicamente; raccolta di tutte le informazioni tecniche in merito alla violazione;
- **RPD** Gestione della procedura di concerto con il RTDP con particolare riferimento alla notifica al Garante;
- **RTDP** Gestione della presente procedura di concerto con il RPD, supervisione e chiusura della stessa.

5. MODALITÀ ESECUTIVE

5.1. Individuazione della violazione

Le violazioni dei dati personali possono essere classificate in base ai seguenti tre principi di sicurezza delle informazioni:

1. **Violazione della riservatezza** – in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
2. **Violazione dell'integrità** – in caso di alterazione non autorizzata o accidentale dei dati personali;
3. **Violazione della disponibilità** – in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.

A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sopra indicati o una combinazione di essi.

Tutti possono rilevare violazioni dei dati personali (di seguito “violazioni”).

5.2. Segnalazione della violazione

Nel caso di violazione dati personali, sia in formato digitale che cartaceo, devono essere osservate le seguenti modalità per la segnalazione:

1. Chi rileva la violazione lo comunica al RAD e per conoscenza al RPD fornendo i dati in suo possesso presenti nel modello semplificato in Allegato 4;
2. Il RAD accerta la reale esistenza dell'incidente, conferma al RPD ed al RTDP l’avvenuta violazione, comunicando le informazioni in proprio possesso.

3. Il RPD, acquisita ogni informazione in merito all'incidente per la sicurezza sui dati personali, inserisce una voce per la descrizione del data breach nel "Registro delle violazioni", come indicato al § 5.7, avviando al contempo le procedure di cui ai successivi §§ 5.3, 5.4 e 5.5.

Nell'Allegato 2 "Scenari di Data Breach" è riportato un elenco esemplificativo di eventi da cui possono derivare violazioni dei dati personali.

5.3. Valutazione del rischio connesso alla violazione

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il RPD (con il supporto di RAD e, se necessario del RTDP) effettua la valutazione del rischio, come di seguito indicato.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- gravità: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Gravità	Impatto della violazione sui diritti e le libertà delle persone coinvolte: ▪ Basso: nessun impatto ▪ Medio: impatto poco significativo, reversibile ▪ Alto: impatto significativo, irreversibile
Probabilità	Possibilità che si verifichino uno o più eventi temuti ▪ Basso: l'evento temuto non si manifesta ▪ Medio: l'evento temuto potrebbe manifestarsi ▪ Alto: l'evento temuto si è manifestato

		Gravità		
		A	M	B
Probabilità	A			
	M			
	B			

Rischio	Descrizione	Notifica Autorità	Comunicazio
	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

- tipo di violazione, secondo quanto specificato al § 5.1;
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori, categorie svantaggiate);
- particolarità dei responsabili del trattamento (es. personale sanitario);
- numero degli interessati.

5.4. Fasi e procedura di valutazione e comunicazione

1) Il RPD stima la gravità e la probabilità della violazione e classifica il rischio;
2) Il RPD, previa condivisione della valutazione con il RTDP, documenta la decisione presa a seguito della valutazione del rischio nel "Registro delle violazioni":
    a. Nel caso in cui il rischio sia considerato non elevato e non si ritenga necessario procedere con la comunicazione, il RPD specifica la giustificazione per tale scelta.
    b. Nel caso il rischio lo richieda, il RPD procede alla notifica della violazione (§ 5.5)
3) Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati dal RPD e tale documentazione è conservata come da § 7.
4) Al fine di attestare il momento in cui si è venuti a conoscenza della violazione, il RPD segnala la violazione a mezzo email al Titolare del trattamento IRSAP, nella persona del legale rappresentante, inviando adeguate informazioni circa la sua natura e gli esiti della valutazione del rischio di cui sopra, nonché anticipando che sta procedendo alla notifica al Garante.

5.5. Notifica della violazione dei dati personali all'autorità di controllo

La normativa prevede che, non appena si viene a conoscenza di una violazione dei dati personali che presenti un rischio di qualsiasi livello superiore al livello "basso" per i diritti e le libertà delle persone coinvolte, è obbligatorio effettuare la notifica all'Autorità.

Per le violazioni così identificate, il RPD con il supporti del RAD, redige il documento di notifica della violazione, compilando l'apposito modello presente sul sito dell'Autorità, procedendo alla notificazione secondo le modalità stabilite da quest'ultima.

L'invio avviene entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza secondo le modalità dio cui al § 5.4.

La notifica all'Autorità di controllo che non sia stata effettuata entro 72 ore, deve essere corredata altresì dei motivi del ritardo.

Il documento di notifica contiene almeno i seguenti elementi:

- la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione;
- i motivi del ritardo, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore;

- eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

5.6. Comunicazione della violazione dei dati personali a interessato/i

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, come valutato secondo quanto indicato al § 5.3, il RPD comunica la violazione all'interessato.

La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione contiene almeno i seguenti elementi:

- la natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione.

Lo schema di comunicazione è riportato in Allegato 3.

Per la comunicazione, è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali email, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

5.7. Documentazione della violazione

Per ogni violazione di cui sia accertata l'esistenza, RPD compila il "Registro delle violazioni", che riporta:

- numerazione progressiva;
- data di rilevazione;
- area/processo interessato dalla violazione;
- descrizione della violazione;
- categorie di interessati in questione;
- numero approssimativo di interessati in questione;
- categorie dei dati personali in questione;
- numero approssimativo di registrazioni dei dati personali in questione;

- cause della violazione;
- conseguenze della violazione;
- misure per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi, con indicazione delle responsabilità e dei tempi per l'attuazione delle misure;
- necessità della notifica alla Autorità e data/ora della stessa, ove applicabile;
- necessità della comunicazione all'interessato e data/ora della stessa, ove applicabile;
- verifica dell'attuazione delle misure;
- verifica dell'efficacia delle misure.

Ad integrazione di quanto riportato nel registro, RPD raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

5.8. Coinvolgimento responsabili e/o titolari autonomi del trattamento

Qualora siano identificati responsabili e/o titolari autonomi del trattamento, sulla base di quanto precedentemente stabilito a mezzo di idonea "Nomina di responsabile del trattamento" ovvero "clausola privacy", il RPTD ed il RPD concorda con i responsabili del trattamento o titolari autonomi le modalità per la gestione della violazione, nonché degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, al fine di garantire il rispetto dei termini di notifica e di comunicazione.

6. ARCHIVIAZIONE

Gli allegati "Notifica" e "Comunicazione" e tutti i documenti relativi alle notifiche ed alle comunicazioni sono archiviati dal RPD, nonché sul sistema di archiviazione documentale e/o digitale di IRSAP dal RPTD.

Il "Registro delle violazioni" è archiviato dal RPD, nonché sul sistema di archiviazione documentale e/o digitale di IRSAP dal RPTD.

7. ALLEGATI

Allegato 1 - Registro delle violazioni;

Allegato 2 – Scenari di Data breach;

Allegato 3 – Comunicazione all'interessato;

Allegato 4 – Modello semplificato.

Esempio	**Notifica all'Autorità**	**Comunicazione agli interessati**	**Note**
Il Titolare conserva il backup di un archivio di dati personali criptati su una chiave USB	NO	NO	Per tutto il tempo in cui i dati sono criptati con uno stato di algoritmi sempre aggiornati, i backup dei dati esistono in un'unica chiave che non è compromessa, e i dati possono essere conservati periodo di tempo corretto questo non può essere considerato violazione da riportare
Il titolare gestisce un servizio on line. A seguito di un attacco informatico su quel servizio, i dati personali dei suoi utenti sono stati trafugati. Il Titolare ha utenti in un singolo stato membro	Sì, riferire all'autorità di controllo se c'è una probabile conseguenza per gli individui	Sì, riferire agli interessati, in base alla natura dei dati personali coinvolti, se la gravità delle probabili conseguenze per gli	
Una breve interruzione di corrente di qualche minuto di durata presso il call center del Titolare che comporta che gli utenti non sono in grado di contattare il Titolare e accedere alla loro documentazione	NO	NO	Questa non è una violazione da notificare, tuttavia è un incidente registrabile secondo l'art. 33(5). Appropriata documentazione sull'evento dovrebbe essere mantenuta dal Titolare
Un Titolare subisce un attacco informatico ransomware per cui tutti i dati sono decriptati. Non sono disponibili backup e i dati non posso essere recuperati. In fase di investigazione, risulta chiaramente che l'unica caratteristica del ransomware era di decriptare i dati e che non c'era	Sì, riferire all'autorità di controllo, se ci sono probabili conseguenze per gli individui poiché in questo caso c'è perdita di disponibilità.	Sì, riferire agli individui, in base alla natura dei dati interessati e alla possibile conseguenza della mancanza di disponibilità dei dati, quali possono essere le possibili conseguenze.	Se c'è un backup disponibile e i dati possono essere conservati per un tempo limitato, questo potrebbe non essere riferito all'autorità di controllo o agli individui poiché non ci sarebbe mancanza definitiva di disponibilità o confidenzialità. Comunque, se l'autorità di controllo viene a conoscenza di un

altro malware presente nel sistema.			incidente per altre vie, può considerare un indagine per valutare la bontà l'adempimento rispetto ai più ampi requisiti di sicurezza in base all'art. 32
Un individuo contatta il call center di una banca per riferire di una violazione di dati. L'individuo ha ricevuto l'estratto conto mensile di qualcun altro. Il titolare intraprende una piccola indagine (es. che si risolve in 24 ore) e ritiene con ragionevole sicurezza che c'è stata violazione dei dati e che il problema sul sistema può o potrà coinvolgere altri individui.	SÌ	Solo agli individui interessati viene notificato se c'è alto rischio ed è chiaro che non riguarda altri.	Se, dopo un'ulteriore indagine si riscontra che l'evento riguarda più interessati, si deve aggiornare l'Autorità di controllo e il Titolare notifica l'evento anche agli altri interessati coinvolti se c'è alto rischio per loro.
Una mail di direct marketing viene inviata a destinatari nei campi "a" o "cc", consentendo così ad ogni destinatario di vedere l'indirizzo mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se sono coinvolti un gran numero di individui e se sono rivelati dati sensibili (es. nella mailing list di uno psicoterapeuta) o se altri fattori presentano alti rischi (es. la mail contiene le password, ecc.).	Sì, riferire agli individui in base allo scopo ed al tipo di dati personali coinvolti ed alla gravità delle possibili conseguenze.	La notifica può non essere necessaria se nessun dato sensibile viene rivelato e se viene rivelato solo
Hardware Utilizzo di chiavette o dischi USB inappropriati per la sensibilità delle informazioni, uso o trasporto di hardware sensibile per scopi personali, il disco rigido contenente le informazioni viene utilizzato per	Sì, riferire all'autorità di controllo se c'è una probabile conseguenza per gli individui	Sì, riferire agli interessati, in base alla natura dei dati personali coinvolti, se la gravità delle probabili conseguenze per gli interessati è alta	La notifica può non essere necessaria se nessun dato sensibile viene rivelato e se viene rivelato solo un minimo numero di indirizzi mail.

uno scopo non previsto (ad esempio per trasportare altri dati ad un fornitore, per trasferire altri dati da un database all'altro, ecc.)			
Hardware Osservazione di uno schermo ad insaputa dell'utilizzatore in un treno, fotografia di uno schermo, geolocalizzazione di un hardware, captazione a distanza di segnali elettromagnetici	Intervento del RPD		
Hardware Tracciatura con un keylogger, rimozione di un componente hardware, connessione di un dispositivo (es. chiave USB) per avviare un sistema operativo o recuperare i dati	Intervento del RPD		
Hardware Furto di un laptop in una camera d'albergo, furto di un telefono cellulare professionale da parte di un borseggiatore, recupero di materiale o supporti da rottamare, perdita di un supporto di memorizzazione elettronico, non cancellazione di dati da materiale o supporti venduti o ceduti a terzi	Intervento del RPD		
Software Ricerca di contenuti, incrocio di dati illegittimo, elevazione di privilegi, cancellazione di tracce, invio di	Intervento del RPD		

spam dal sistema di messaggistica, messa fuori uso della rete			
Software Scansione di indirizzi e porte di rete, raccolta di dati di configurazione, studio del codice sorgente per determinare errori sfruttabili, test delle risposte del database a query dannose	Intervento del RPD		
Software Tracciatura con un keylogger, contagio da codice dannoso, installazione di uno strumento di controllo remoto, sostituzione di un componente con un altro durante un aggiornamento, un'operazione di manutenzione o un'installazione (parti del codice o dell'applicazione sono installati o sostituiti)	Intervento del RPD		
Rete di dati Intercettazione di flussi di dati sulla rete Ethernet, acquisizione di dati su una rete wireless	Intervento del RPD		
Persone Divulgazione involontaria durante la conversazione, ascolto delle conversazioni in una sala riunioni con apparecchiature di amplificazione	Intervento del RPD		
Persone Influenza (phishing, ingegneria sociale, corruzione), pressione	Intervento del RPD		

(ricatto, molestie morali)			
Persone Assunzione di dipendenti, cambio di incarico, acquisizione di tutta o parte dell'organizzazione	Intervento del RPD		
Documenti cartacei Lettura, fotocopia, fotografia	Intervento del RPD		
Documenti cartacei Furto di documentazione negli uffici, furto di posta nella cassetta postale, recupero di documenti gettati nei rifiuti	Intervento del RPD		
Trasmissione di documenti cartacei Lettura di libri firma in circolazione, riproduzione di documenti in transito	Intervento del RPD		
Hardware Aggiunta di hardware incompatibile che determina un malfunzionamento, rimozione dell'hardware essenziale per il corretto funzionamento di un'applicazione	Intervento del RPD		
Software Modifiche non desiderate in un database, cancellazione di file utili per il corretto funzionamento, errore di manipolazione che porta alla modifica dei dati	Intervento del RPD		
Software Errore durante l'aggiornamento, la configurazione o la manutenzione,	Intervento del RPD		

contagio da codice malevolo, sostituzione di un componente con un altro			
Rete di dati Attacco “man-in-the-middle” per modificare o aggiungere dati al traffico di rete; replay attack (rinvio di dati intercettati)	Intervento del RPD		
Documenti cartacei Modifica dei numeri in una documento, sostituzione di un documento con un falso	Intervento del RPD		
Trasmissione di documenti cartacei Modifica di una nota all’insaputa dell’estensore, sostituzione di un libro firma con un altro, invio multiplo di lettere contraddittorie	Intervento del RPD		
Hardware Archiviazione di file personali, utilizzo per scopi personali	Intervento del RPD		
Hardware Unità di memoria piena, interruzione di corrente, sfruttamento eccessivo delle capacità di elaborazione, surriscaldamento, eccessiva temperatura, attacco “Denial of Service”	Intervento del RPD		
Hardware Aggiunta di hardware incompatibile che porta ad un malfunzionamento, rimozione di un componente			

necessario per il funzionamento del sistema			
Hardware Inondazioni, incendi, atti vandalici, degradazione dovuta all'usura naturale, malfunzionamento di un dispositivo di memorizzazione			
Hardware Furto di un laptop, perdita di un telefono cellulare, rottamazione di un supporto o di attrezzature, dischi sottodimensionati che portano ad una moltiplicazione di supporti e alla perdita di alcuni di loro			
Software Cancellazione di dati, utilizzo di software contraffatto o copiato, errore dell'operatore che porta alla cancellazione dei dati			
Software Superamento del dimensionamento del database, inserimento di dati al di fuori dei valori previsti, attacco "Denial of Service"			
Software Errore durante l'aggiornamento, la configurazione o la manutenzione, contagio da codice malevolo, sostituzione di un componente con un altro			

Software Cancellazione di un programma in esecuzione o di codice sorgente, virus, malware “bomba logica”			
Software Non rinnovo della licenza software utilizzata per accedere ai dati, interruzione degli aggiornamenti di sicurezza da parte del produttore, fallimento del produttore, corruzione del modulo di archiviazione contenente i numeri di licenza			
Rete di dati Riduzione della larghezza di banda, download non autorizzato, interruzione dell’accesso a Internet			
Rete di dati Interruzione del cablaggio, scarsa ricezione della rete Wi-Fi, ossidazione dei cavi			
Persone Decesso, pensionamento, cambio di incarico, fine del contratto o licenziamento, acquisizione di tutta o parte dell’organizzazione			
Documenti cartacei Cancellazione graduale nel tempo, cancellazione volontaria di parti di un testo, riutilizzo di documenti per prendere appunti estranei al trattamento, uso di quaderni per			

fare qualcos'altro			
Documenti cartacei Invecchiamento di documenti archiviati, bruciatura di documenti durante un incendio			
Documenti cartacei Furto di documenti, perdita di documenti durante un trasloco, smaltimento			
Trasmissione di documenti cartacei Sovraccarico dei servizi postali, sovraccarico di un processo di convalida			
Trasmissione di documenti cartacei Taglio del flusso a seguito di una riorganizzazione, blocco della posta a causa di uno sciopero			
Trasmissione di documenti cartacei Modifica delle modalità di spedizione, riassegnazione di uffici o locali, riorganizzazione della spedizione di documenti cartacei, cambio della lingua utilizzata			
Trasmissione di documenti cartacei Riorganizzazione che elimina un processo, scomparsa di un corriere di documenti, perdita delle poste			

Allegato 3

Registro dei trattamenti IRSAP

REGISTRO DEI TRATTAMENTI

N° Rev.	Data Revisione	Descrizione	Firma Responsabile
00	_____	Prima Emissione	

SOMMARIO

Allegato 3

Registro dei trattamenti IRSAP

Allegato 3

Registro dei trattamenti IRSAP

ESTREMI DEL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati personali è _____ (di seguito anche soltanto "Titolare" e/o "Ente"), p. i.v.a. _____ e c.f. _____.

Il Titolare del trattamento può essere contattato presso:

a) via _____;
b) numero _____;
c) all'indirizzo mail ordinaria _____;
d) all'indirizzo pec _____.

Il Titolare ha provveduto a nominare un Responsabile per la Protezione dei Dati: _____ nella persona di _____.

Allegato 3

Registro dei trattamenti IRSAP

INDICAZIONE DELLE TIPOLOGIE E DELLE FINALITÀ DEI TRATTAMENTI

ID	TIPOLOGIA TRATTAMENTO
A	SELEZIONE DEL PERSONALE Dati personali, anche particolari (c.d. "sensibili"), sono raccolti al fine di trattare i dati personali nell'ambito delle procedure di selezione del personale;
B	GESTIONE RAPPORTO DI LAVORO Dati personali, anche particolari (c.d. "sensibili"), sono raccolti al fine di trattare i dati personali dei dipendenti nell'ambito del rapporto di lavoro. In particolare i predetti dati sono trattati per finalità di: **1.** assunzione; **2.** esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi: **2.1.** stabiliti dalla legge o da contratti collettivi; **2.2.** di gestione, pianificazione e organizzazione del lavoro; **2.3.** formazione professionale; **2.4.** servizi di controllo interno (anche ai sensi dell'art. 4 dello Statuto dei lavoratori); **2.5.** di parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro; **2.6.** ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro; **3.** cessazione del rapporto di lavoro.
C	SISTEMA VIDEOSORVEGLIANZA I dati personali dei dipendenti nell'ambito del sistema di videosorveglianza per finalità relativa ad esigenze organizzative e produttive; sicurezza del lavoro; tutela del patrimonio aziendale.
D	SISTEMI INFORMATICI E TELEMATICI I dati personali dei dipendenti nell'ambito dell'utilizzo dei sistemi informatici e telematici (quali strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa) per finalità di esigenze organizzative e produttive; sicurezza del lavoro; tutela del patrimonio aziendale.
E	RAPPORTI PROFESSIONALI FORNITORI I dati personali dei fornitori sono trattati per finalità di: **1.** _____: **2.** inoltrare comunicazioni di vario genere e con diversi mezzi di comunicazione (telefono, telefono cellulare, sms, email, fax, posta cartacea); **3.** formulare richieste, evadere richieste e/o proposte pervenute;

Registro dei trattamenti IRSAP

	4. scambiare informazioni finalizzate all'esecuzione del rapporto contrattuale, ivi comprese le attività pre e post contrattuali e di fatturazione.
G	RAPPORTI CON IL PUBBLICO I dati personali sono trattati per finalità di: 1. _____. 2. _____. 3. _____. 1. _____.
H	GESTIONE VISITATORI I dati personali dei visitatori che accedono all'area amministrativa, che accedono alle aree di produzione o che accedono a specifiche attività, sono trattati per finalità relativa ad esigenze organizzative e produttive; sicurezza del lavoro; tutela del patrimonio aziendale
I	GESTIONE REGISTRAZIONE DELLE PRESENZE I dati personali degli interessati (dipendenti) sono trattati per finalità relative alla gestione del rapporto di lavoro con particolare riferimento alle presenze, assenze, permessi e ferie dei dipendenti all'interno dello stabilimento.
J	GESTIONE RECLAMI E CONTROVERSIE LEGALI I dati personali degli interessati (consumatori) sono trattati per finalità relative alla gestione dei reclami che questi possono inoltrare all'azienda in relazione ai prodotti acquistati, nonché relative alla richiesta di informazioni avanzate dai medesimi interessati
L	GESTIONE RESPONSABILI E CONTITOLARI DEL TRATTAMENTO I dati personali degli interessati (dipendenti, collaboratori, fornitori e agenti) sono trattati per finalità relative alla gestione dei rapporti di lavoro e commerciali sulla base di accordi e relative nomine sottoscritti con fornitori esterni.

Allegato 3

Registro dei trattamenti IRSAP

NOTE
➢ Il titolare del trattamento fa presente che _____. ➢ Il titolare del trattamento fa presente che _____. ➢ Il titolare del trattamento fa presente che _____. ➢ L'analisi del rischio allegata fa riferimento _____. ➢ _____

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "A)" SELEZIONE DEL PERSONALE

Funzione aziendale che svolge il trattamento	Ufficio delle Risorse Umane come da organigramma privacy allegato e relative istruzioni interne.
Categoria degli interessati	Candidati

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
Anagrafiche generali; Curriculum vitae		No

Mezzi di trattamento
I dati personali vengono trattati in formato elettronico ed in formato cartaceo.

Base giuridica dei dati trattati
Invio spontaneo del curriculum (Dlgs 196/2016 e D.lgs 101/2018); Ricezione curriculum tramite agenzia di somministrazione e /o selezione (contratto) o tramite piattaforma web; Legittimo interesse del datore (art. 6, par. 1, lett. f del GDPR); Nel caso il curriculum contenga dati sensibili viene fatto sottoscrivere un consenso esplicito.
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di conservare presso i propri data base possibili candidature che pur risultando -al momento della valutazione- valide, non sono considerabili ai fini di una immediata assunzione; tuttavia potrebbero esserlo in futuro.

Tempi di conservazione
I dati personali dei candidati assunti seguono i tempi di conservazione dei dipendenti. I dati personali dei candidati non idonei vengono cancellati. I dati personal dei candidati idonei ma che non possono essere assunti vengono conservati per tre anni

Allegato 3

Registro dei trattamenti IRSAP

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi
I dati personali sono comunicati, in stretta relazione alle finalità sopra indicate, al personale dell'ufficio Risorse Umane e della Direzione di . I dati non sono trasferiti verso Paesi extra UE.

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	_____.
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio _____ in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	_____	_____
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	_____	_____.
Danneggiamento dati conservati in cartaceo	_____	_____
Danneggiamento dati conservati in digitale	_____	_____
Indisponibilità dei dati conservati in cartaceo	_____	_____
Indisponibilità dei dati conservati	_____ _____	_____

Allegato 3

Registro dei trattamenti IRSAP

in digitale		

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "B)" GESTIONE RAPPORTO DI LAVORO	
Funzione aziendale che svolge il trattamento	Ufficio delle Risorse Umane, nonché i responsabili Area per i propri sottoposti come da organigramma privacy allegato. Sussistono istruzioni interne
Categoria degli interessati	Dipendenti

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
Anagrafiche generali; - Retribuzioni, compensi, paghe; - Mansioni, livello contrattuale, incarichi; - Esperienze lavorative; - Presenze, permessi, ferie; - Dati di natura valutativa; - Archivi immagini; - Video, filmati; - Hobbies, interessi; - Composizione del nucleo familiare; - Eventuali procedure esecutive, cessioni del quinto e deleghe di pagamento; - Eventuali assegni familiari.	- Origine razziale, etnica - Convinzioni religiose, filosofiche; - Convinzioni politiche o sindacali; - Malattia; - Infortuni; - Disabilità; - Invalidità; - Stato di gravidanza e/o maternità	No

Mezzi di trattamento
I dati personali vengono trattati sia in formato elettronico che cartaceo

Base giuridica dei dati trattati
- Contratto di assunzione; - Consenso esplicito

Registro dei trattamenti IRSAP

- CCNL di riferimento; - L. 300/70; - D.Lgs. n. 151/2001; - D.Lgs. n. 81/2008, succ. int. D.Lgs. n. 106/2009); - D.Lgs. del 11 aprile 2006, n. 198; - Legittimo interesse del datore (art. 6, par. 1, lett. f del GDPR); - D.Lgs 196/2003; - Regolamento 679/2016 - D.Lgs 101/2018 - Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018 - Linee guida sul trattamento di dati personali dei lavoratori privati - 23 novembre 2006 - Consenso
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di dover trattare detti dati personali al fine del perseguimento dello scopo sociale dell'impresa, a tutela dei rapporti di lavoro e del patrimonio aziendale, nonché per difendere un diritto in giudizio in caso di contestazioni e/o illeciti civili e/o penali.

Tempi di conservazione
I dati vengono conservati durante l'intero rapporto lavorativo, e per dieci anni a decorrere dalla data di cessazione: - per adempiere agli obblighi legislativi in materia di conservazione dei documenti fiscali e contabili aziendali; in ottemperanza ai criteri di prescrizione ordinaria di cui al codice civile.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi
I dati personali saranno comunicati, in stretta relazione alle finalità sopra indicate, oltre che ai dipendenti di debitamente autorizzati, anche alle seguenti categorie di soggetti: • Amministratore di Sistema, individuato nominalmente nel Regolamento sull'utilizzo degli strumenti informatici; • Istituto Nazionale della Previdenza Sociale, al fine dell'adempimento di ogni obbligo previdenziale, assistenziale e assicurativo; • Istituti bancari, al fine del pagamento della retribuzione e di ogni indennità o rimborsi; • Istituti bancari e o creditori in caso di richieste di azioni legali di recupero crediti, nei limiti strettamente necessari alle disposizioni di

Registro dei trattamenti IRSAP

legge in materia; • Medico competente e/o istituzioni specializzate esterne, al fine della valutazione dell'idoneità sanitaria alle mansioni attribuite; • Responsabile del servizio di prevenzione e protezione, ove fosse indicato un professionista esterno, per gli adempimenti di competenza; • Studio di consulenza del lavoro ai fini della determinazione della retribuzione, della gestione della posizione con gli enti di previdenza, dello studio e risoluzione di eventuali problemi giuridici relativi alla posizione contrattuale, o in relazione ad obblighi normativi che la è tenuta a rispettare; • Consulenti legali aziendali, ai fini dello studio e risoluzione di eventuali problemi giuridici relativi alla Sua posizione contrattuale, o in relazione ad obblighi normativi e/o contrattuali che la è tenuta a rispettare; • Compagnie assicurative e/o fondi e/o casse di assistenza o previdenza con i quali il Titolare intrattiene rapporti o convenzioni a favore dei dipendenti anche sulla base di quanto previsto dalla legge o dal CCNL; • Organizzazioni sindacali per le comunicazioni di legge; • Altri istituti della Pubblica Amministrazione (ad esempio l'INAIL) per le specifiche pratiche di loro stretta competenza, ivi compresi i centri di assistenza fiscale; • Società e/o fondi di formazione con i quali la intrattiene rapporti di collaborazione ai fini della gestione erogazione della formazione del personale; • I clienti e o partner commerciali con i quali la Società intrattiene rapporti di collaborazione, ai fini dello svolgimento delle attività e delle mansioni correlate; • I soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative internazionali.	
Individuazione dei contitolari, dei titolari autonomi e dei responsabili del trattamento	Il consulente del lavoro è considerato responsabile del trattamento e con lo stesso è stato sottoscritto uno specifico accordo di designazione per garantire il pieno rispetto dei diritti dell'interessato. Il medico competente è considerato titolare autonomo del trattamento.
I dati personali non saranno trasferiti verso Paesi extra UE.	

Allegato 3

Registro dei trattamenti IRSAP

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	_____).
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio MEDIO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue. Si precisa che il livello di rischio tiene conto che i dati vengono trattati anche da soggetti esterni (consulenti nominati responsabili del trattamento) sulla cui attività il titolare del trattamento non può avere un controllo pieno e diretto.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	_____	_____
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	_____	_____.
Danneggiamento dati conservati in cartaceo	_____	_____
Danneggiamento dati conservati in digitale	_____	_____
Indisponibilità dei dati conservati in cartaceo	_____	_____
Indisponibilità dei dati conservati in digitale	_____	_____

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "C)" SISTEMA VIDEOSORVEGLIANZA

Funzione aziendale che svolge il trattamento	Ufficio tecnico, portineria
Categoria degli interessati	Sistema di videosorveglianza

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
Immagini	No	No

Mezzi di trattamento
I dati personali vengono trattati in formato elettronico

Base giuridica dei dati trattati
- Stato dei Lavoratori (Art. 4 L. 300/70) - Autorizzazione della Direzione Provinciale del Lavoro del 2011 - Contratto di affitto d'azienda da S.p.A. a International - Provvedimento in materia di videosorveglianza, dell'8 aprile 2010 emesso dal Garante per il trattamento dei dati personali

Tempi di conservazione
I tempi di conservazione sono di 72 ore e sono disciplinate dall'autorizzazione della Direzione provinciale del lavoro e dal Regolamento interno sul sistema di videosorveglianza

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
• I dati non vengono comunicati all'esterno	
Individuazione dei contitolari e dei responsabili del trattamento	Sono stati individuati e nominati il Responsabile e l'addetto al sistema di videosorveglianza.
I dati personali non saranno trasferiti verso Paesi extra UE.	

Allegato 3

Registro dei trattamenti IRSAP

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	In considerazione dell'attività svolta dal titolare del trattamento e degli strumenti automatizzati che lo stesso utilizza al fine del trattamento dei dati personali si è proceduto ad un'analisi del rischio informatico redatta a seguito di consulenza esterna . Si allega altresì il rapporto di un'analisi del rischio generale basata sui controlli indicati dalla norma internazionale ISO 27001:2013 (All. C).
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio MEDIO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	Non sussiste un trattamento cartaceo dei dati personali	N/A
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Il sistema di registrazione è chiuso a chiave conservate dai soli Responsabili nominati	Il titolare del trattamento sta attivando le relative procedure di controllo ed ulteriori presidi di sicurezza
Danneggiamento dati conservati in cartaceo	Non sussiste un trattamento cartaceo dei dati personali	N/A
Danneggiamento dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Il sistema viene monitorato periodicamente Sussiste piano anti-incendio	Il titolare del trattamento sta attivando e verificando la necessità di relative procedure di aggiornamento del software
Indisponibilità dei dati conservati in cartaceo	Non sussiste un trattamento cartaceo dei dati personali	N/A

Registro dei trattamenti IRSAP

Indisponibilità dei dati conservati in digitale	I dati sono sempre disponibili e verificati periodicamente	Il titolare del trattamento sta attivando e verificando la necessità di relative procedure di aggiornamento del software

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "D)" SISTEMI INFORMATICI E TELEMATICI	
Funzione aziendale che svolge il trattamento	I Servizi IT della come indicato nell'organigramma allegato
Categoria degli interessati	Sistema informatico e telematico aziendale

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- credenziali di accesso ai sistemi; - dati di log; - database e gestionali di lavoro; - client mail; - software navigazione internet;		

Mezzi di trattamento
I dati personali vengono trattati in formato elettronico

Base giuridica dei dati trattati
- Contratto di assunzione - Statuto del Lavoratori (art. 4 L. 300/70) - Provvedimento in materia di internet e utilizzo mail emesso dal 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), così modificato in base al provvedimento del 25 giugno 2009. - Regolamento Europeo n. 679/16 art. 32; - Legittimo interesse (art. 6, par. 1, lett. f del GDPR)
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda

sulla necessità da parte di di organizzare e svolgere l'intera attività produttiva della Società e tutelarne l'integrale e continuo funzionamento, nonché a proteggere il patrimonio aziendale.

Tempi di conservazione
I tempi di conservazione sono diversi a seconda della tipologia di interessato di processi aziendali a cui si riferiscono. Si rimanda al Regolamento sull'utilizzo degli strumenti informatici, alla Nomina ad amministratore di sistema e responsabile violazione dati, alla nomina di incarico di custode delle credenziali.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
Il sistema informatico viene gestito interamente dall'Ufficio Servizi IT anche in fase di manutenzione tranne per problematiche connesse ai fornitori di servizio di connessione ovvero problemi strutturali. In tali casi gli operatori intervenuti vengono adeguatamente incaricati ed istruiti per la corretta gestione dei dati personali che potrebbero dover trattare nell'adempimento delle proprie mansioni. I temi di conservazione dei log di sistema sono conformi a quanto stabilito dal provvedimento emesso dal Garante nel 2008 in materia di Amministratori di sistema	
Individuazione dei contitolari e dei responsabili del trattamento	Il servizio è gestito internamente
I dati personali non saranno trasferiti verso Paesi extra UE.	

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	In considerazione dell'attività svolta dal titolare del trattamento e degli strumenti cartacei ed automatizzati che lo stesso utilizza al fine del trattamento dei dati personali si è proceduto ad un'analisi del rischio informatico redatta a seguito di consulenza esterna .
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio articolato MEDIO a seconda del trattamento di riferimento; ciò in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati da tabella che segue.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	**Misura di sicurezza**	**Analisi**

Registro dei trattamenti IRSAP

Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	N/A	N/A
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza (v. note ad inizio documento)
Danneggiamento dati conservati in cartaceo	N/A	N/A
Danneggiamento dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Sussiste un sistema anti incendio Sussiste un sistema di videosorveglianza	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza (v. note ad inizio documento)
Indisponibilità dei dati conservati in cartaceo	N/A	N/A
Indisponibilità dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza (v. note ad inizio documento)

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "E)" RAPPORTI COMMERCIALI FORNITORI

Funzione aziendale che svolge il trattamento	Il relativo ufficio interno di riferimento della come indicato nell'organigramma
Categoria degli interessati	Fornitori (imprese individuali, legali rappresentanti o dipendenti di società)

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- nome e cognome; - indirizzo mail; - numeri di telefono; - dati fatturazione: - mansione ricoperta	No	No

Mezzi di trattamento
I dati personali vengono trattati sia in formato elettronico che cartaceo

Base giuridica dei dati trattati
- Contratto di fornitura - normativa fiscale e tributaria - Legittimo interesse (art. 6, par. 1, lett. f del GDPR)
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di dover trattare detti dati personali al fine del perseguimento dello scopo sociale dell'impresa, all'esecuzione dei contratti di fornitura e dei rapporti commerciali con i partner, nonché di difendere i propri diritti in giudizio in caso di contestazioni.

Tempi di conservazione
I dati vengono conservati durante l'intero rapporto commerciale, e per dieci anni dalla data di cessazione:

- per adempiere agli obblighi legislativi in materia di conservazione dei documenti fiscali e contabili aziendali; - in ottemperanza ai criteri di prescrizione ordinaria di cui al codice civile.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
I dati personali saranno comunicati, oltre ai dipendenti della debitamente autorizzati, in stretta relazione alle finalità sopra indicate, anche ai seguenti soggetti o categorie di soggetti: - i clienti e/o partner con i quali la Società intrattiene rapporti di collaborazione, ai fini dell'organizzazione ed esercizio dell'attività imprenditoriale; - uffici interni di , debitamente autorizzati al trattamento; - lo studio commercialista, per le attività fiscali, tributarie e contabili; - lo studio legale per la risoluzione delle questioni giuridiche attinenti al rapporto commerciale; - i soggetti comunque autorizzati ad accedervi in ragione di disposizioni di leggi e dei regolamenti nazionali ed internazionali.	
Individuazione dei contitolari e dei responsabili del trattamento	Lo studio legale e lo studio commercialista sono nominati responsabili del trattamento.
I dati personali non saranno trasferiti verso Paesi extra UE.	

Dichiarazione nel rispetto dell'art. 14 comma 5, lett. a) e b)
Le informative ai sensi dell'art. 14 indirizzate ai dipendenti, delle società fornitrici, i cui dati personali vengono trattati da non vengono comunicate in quanto, in considerazione del continuo cambiamento del personale da parte delle società fornitrici e la molteplicità dei contratti commerciali sottoscritti dal titolare del trattamento, richiederebbe uno sforzo sproporzionato sia in termini di gestione che di costi. A ciò deve altresì precisarsi che comunque gli interessati dispongono già delle informazioni in quanto sono stati informati dai propri datori di lavoro.

Allegato 3

Registro dei trattamenti IRSAP

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	In considerazione dell'attività svolta dal titolare del trattamento e degli strumenti cartacei ed automatizzati che lo stesso utilizza al fine del trattamento dei dati personali si è proceduto ad un'analisi del rischio informatico redatta a seguito di consulenza esterna . Si allega altresì il rapporto di un'analisi del rischio generale basata sui controlli indicati dalla norma internazionale ISO 27001:2013 (All. E).
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio BASSO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue. Si precisa che il livello di rischio tiene conto che i dati vengono trattati anche da soggetti esterni sulla cui attività il titolare del trattamento non può avere un controllo pieno e diretto.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	Sussiste un controllo degli accessi (portineria) ma non un controllo specifico ai singoli archivi ed ai locali cui sono collocati che non hanno serratura a chiave. Lo stabilimento è presidiato da vigilanza anche notturna. Sussiste un sistema di allarme. Sussiste un sistema di videosorveglianza	Sussistono politiche di accesso e gestione. Il titolare sta attivando ulteriori misure di sicurezza
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Con i consulenti esterni sono state redatte apposite istruzioni. Sussiste un sistema di allarme. Sussiste un sistema di videosorveglianza	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza

Registro dei trattamenti IRSAP

Danneggiamento dati conservati in cartaceo	I fascicoli cartacei sono conservati adeguatamente ed in armadi sicuri Sussiste un piano anti incendio Sussiste un sistema di videosorveglianza	Si sta valutando se adottare misure maggiormente incisive
Danneggiamento dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Sussiste un piano anti incendio Con i consulenti esterni sono state redatte apposite istruzioni.	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza
Indisponibilità dei dati conservati in cartaceo	I fascicoli cartacei sono sempre disponibili Con i consulenti esterni sono state redatte apposite istruzioni.	Sussistono politiche di accesso e gestione
Indisponibilità dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Con i consulenti esterni sono state redatte apposite istruzioni.	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "F)" RAPPORTI COMMERCIALI AGENTI/PROCACCIATORI DI COMMERCIO	
Funzione aziendale che svolge il trattamento	Il relativo ufficio interno di riferimento della , come indicato nell'organigramma
Categoria degli interessati	Agenti di commercio

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- nome e cognome; - indirizzo mail; - numeri di telefono; - dati fatturazione:	No	No

Mezzi di trattamento
I dati personali vengono trattati sia in formato elettronico che cartaceo

Base giuridica dei dati trattati
- Contratto di fornitura - Legittimo interesse (art. 6, par. 1, lett. f del GDPR) - Consenso informato - D.Lgs 101/2018
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di dover trattare detti dati personali al fine del perseguimento dello scopo sociale dell'impresa, nonché di difendere i propri diritti in giudizio in caso di contestazioni e/o illeciti civili e/o penali.

Tempi di conservazione
I dati vengono conservati durante l'intero rapporto commerciale, e per dieci anni dalla data di cessazione:

Registro dei trattamenti IRSAP

- per adempiere agli obblighi legislativi in materia di conservazione dei documenti fiscali e contabili aziendali; - in ottemperanza ai criteri di prescrizione ordinaria di cui al codice civile.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
I dati personali saranno comunicati, oltre ai dipendenti della debitamente autorizzati, in stretta relazione alle finalità sopra indicate, anche ai seguenti soggetti o categorie di soggetti: - i clienti e o partner con i quali la Società intrattiene rapporti di collaborazione, ai fini dell'organizzazione ed esercizio dell'attività imprenditoriale; - uffici interni di , debitamente autorizzati al trattamento; - lo studio commercialista, per le attività fiscali, tributarie e contabili; - lo studio legale per la risoluzione delle questioni giuridiche attinenti al rapporto commerciale; - i soggetti comunque autorizzati ad accedervi in ragione di disposizioni di leggi e dei regolamenti nazionali ed internazionali.	
Individuazione dei contitolari e dei responsabili del trattamento	Il consulente legale e lo studio commercialistico sono nominati responsabili del trattamento
I dati personali non saranno trasferiti verso Paesi extra UE.	

Allegato 3

Registro dei trattamenti IRSAP

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	In considerazione dell'attività svolta dal titolare del trattamento e degli strumenti cartacei ed automatizzati che lo stesso utilizza al fine del trattamento dei dati personali si è proceduto ad un'analisi del rischio informatico redatta a seguito di consulenza esterna . Si allega altresì il rapporto di un'analisi del rischio generale basata sui controlli indicati dalla norma internazionale ISO 27001:2013 .
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio BASSO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue. Si precisa che il livello di rischio tiene conto che i dati vengono trattati anche da soggetti esterni sulla cui attività il titolare del trattamento non può avere un controllo pieno e diretto.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	Sussiste un controllo degli accessi (portineria) ma non un controllo specifico ai singoli archivi ed ai locali cui sono collocati che non hanno serratura a chiave. Lo stabilimento è presidiato da vigilanza anche notturna. Sussiste un sistema di allarme. Sussiste un sistema di videosorveglianza	Sussistono politiche di accesso e gestione. Il titolare sta attivando ulteriori misure di sicurezza.
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Con i consulenti esterni sono state redatte apposite istruzioni.	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di dicurezza
Danneggiamento dati conservati in cartaceo	I fascicoli cartacei sono conservati adeguatamente ed in armadi sicuri	Si sta valutando se adottare misure maggiormente incisive

Registro dei trattamenti IRSAP

	Con i consulenti esterni sono state redatte apposite istruzioni. Sussiste un sistema anti incendio Sussiste un sistema di videosorveglianza	
Danneggiamento dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Con i consulenti esterni sono state redatte apposite istruzioni. Sussiste un piano anti incendio	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza
Indisponibilità dei dati conservati in cartaceo	I fascicoli cartacei sono sempre disponibili Con i consulenti esterni sono state redatte apposite istruzioni.	Sussistono politiche di accesso e gestione
Indisponibilità dei dati conservati in digitale	Sussistono alcuni controlli sul sistema informatico Con i consulenti esterni sono state redatte apposite istruzioni.	Il titolare del trattamento sta attivando le relative procedure di controllo e relative misure di sicurezza

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "G)" RAPPORTI CON IL PUBBLICO E LE IMPRESE

Funzione aziendale che svolge il trattamento	Il relativo ufficio interno di riferimento della come indicato nell'organigramma
Categoria degli interessati	Pubblico e imprese

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- nome e cognome; - indirizzo mail; - numeri di telefono; - dati fatturazione; - Codice fiscale; - Importo complessivo delle operazioni effettuate con dettaglio di imponibile; - Imposta; - Importo delle operazioni non imponibili e esenti.		

Mezzi di trattamento
I dati personali vengono trattati sia in formato elettronico che cartaceo

Base giuridica dei dati trattati
- Contratto commerciale ; - Legittimo interesse (art. 6, par. 1, lett. f del GDPR); - Decreto Legge n. 223 del 4 luglio 2006 convertito con legge n. 248 del 04/08/2006
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di dover trattare detti dati personali al fine del perseguimento dello scopo sociale dell'impresa,

all'esecuzione dei contratti di fornitura e dei rapporti commerciali con i partner, nonché di difendere i propri diritti in giudizio in caso di contestazioni.

Tempi di conservazione
I dati vengono conservati durante l'intero rapporto commerciale, e per dieci anni dalla data di cessazione: - per adempiere agli obblighi legislativi in materia di conservazione dei documenti fiscali e contabili aziendali; - in ottemperanza ai criteri di prescrizione ordinaria di cui al codice civile.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
I dati personali saranno comunicati, in stretta relazione alle finalità sopra indicate, ai seguenti soggetti o categorie di soggetti: - i partner con i quali la Società intrattiene rapporti di collaborazione, ai fini strettamente connessi dell'organizzazione ed esercizio dell'attività imprenditoriale; - uffici interni di , debitamente autorizzati al trattamento; - lo studio commercialista, per le attività fiscali, tributarie e contabili; - lo studio legale per la risoluzione delle questioni giuridiche attinenti al rapporto commerciale; - i soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative comunitarie.	
Individuazione dei contitolari e dei responsabili del trattamento	_____
I dati personali non saranno trasferiti verso Paesi extra UE.	

Dichiarazione nel rispetto dell'art. 14 comma 5, lett. a) e b)
Le informative ai sensi dell'art. 14 indirizzate ai dipendenti, delle società clienti, i cui dati personali comuni vendono trattati da in ragione dell'esecuzione del contratto tra la stessa ed i clienti, non vengono comunicate in quanto, in considerazione del continuo cambiamento del personale da parte delle società clienti e la molteplicità dei contratti commerciali sottoscritti dal titolare del trattamento, richiederebbe uno sforzo sproporzionato sia in termini di gestione che di costi. A ciò deve altresì precisarsi che comunque gli interessati dispongono già delle informazioni in quanto sono stati informati dai propri datori di lavoro.

Allegato 3

Registro dei trattamenti IRSAP

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	In considerazione dell'attività svolta dal titolare del trattamento e degli strumenti cartacei ed automatizzati che lo stesso utilizza al fine del trattamento dei dati personali si è proceduto ad un'analisi del rischio informatico redatta a seguito di consulenza esterna . Si allega altresì il rapporto di un'analisi del rischio generale basata sui controlli indicati dalla norma internazionale ISO 27001:2013 (All. G).
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio BASSO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue. Si precisa che il livello di rischio tiene conto che i dati vengono trattati anche da soggetti esterni sulla cui attività il titolare del trattamento non può avere un controllo pieno e diretto.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	_____	_____
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	_____	_____
Danneggiamento dati conservati in cartaceo	_____	_____
Danneggiamento dati conservati in digitale	_____	_____
Indisponibilità dei dati conservati in cartaceo	_____	_____
Indisponibilità dei dati conservati in	_____	_____

Registro dei trattamenti IRSAP

digitale		

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "H)" GESTIONE VISITATORI	
Funzione aziendale che svolge il trattamento	L'ufficio Risorse Umane e l'ufficio portineria della come indicato nell'organigramma
Categoria degli interessati	Visitatori uffici, visitatori aree produzione, visitatori attività

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- nome e cognome; - contatti; - residenza; - qualifica lavorativa; - contatti.		No

Mezzi di trattamento
Cartaceo

Base giuridica dei dati trattati
- Legittimo interesse (art. 6, par. 1, lett. f del GDPR) - consenso esplicito - L. 81/08 - ISO 9001:2015
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di tutelare la sicurezza del patrimonio fisico, logico ed informativo dell'azienda nonché la salute degli interessati e dei consumatori.

Allegato 3

Registro dei trattamenti IRSAP

Tempi di conservazione
I dati vengono conservati per tutto il periodo di permanenza dell'interessato all'interno dei locali aziendali. Vengono eliminati entro trenta giorni a far data dall'accesso del visitatore.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
I dati personali sono trattati dal solo personale all'accettazione e dall'ufficio Risorse Umane, ovvero, nel caso di visitatori delle aree produzione e i visitatori attività anche dal personale a ciò debitamente autorizzato in stretta relazione alle finalità sopra indicate. Potrebbero essere comunicati alle Autorità nei casi previsti da leggi e regolamenti nazionali ed internazionali.	
Individuazione dei contitolari e dei responsabili del trattamento	Nessuno
I dati personali non saranno trasferiti verso Paesi extra UE.	

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	In considerazione dell'attività svolta dal titolare del trattamento e degli strumenti cartacei ed automatizzati che lo stesso utilizza al fine del trattamento dei dati personali si è proceduto ad un'analisi del rischio informatico redatta a seguito di consulenza esterna . Si allega altresì il rapporto di un'analisi del rischio generale basata sui controlli indicati dalla norma internazionale ISO 27001:2013 (All. H).
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio MEDIO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	_____	_____
Perdita, sottrazione, divulgazione,	_____	_____

alterazione, accesso dei dati conservati in digitale		
Danneggiamento dati conservati in cartaceo	_____	_____
Danneggiamento dati conservati in digitale	_____	_____
Indisponibilità dei dati conservati in cartaceo	_____	_____
Indisponibilità dei dati conservati in digitale	_____	_____

Allegato 3

Registro dei trattamenti IRSAP

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "I)" GESTIONE REGISTRAZIONE DELLE PRESENZE	
Funzione aziendale che svolge il trattamento	L'ufficio Risorse Umane e Servizi IT della come indicato nell'organigramma
Categoria degli interessati	Rilevazione delle presenze

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- numero identificativo del badge assegnato al dipendente		No

Mezzi di trattamento
I dati personali vengono trattati in formato elettronico

Base giuridica dei dati trattati
- Legittimo interesse (art. 6, par. 1, lett. f del GDPR) - L. 300/70 - Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018 - Linee guida sul trattamento di dati personali dei lavoratori privati - 23 novembre 2006
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di gestire ed organizzare il lavoro aziendale nonché di tutelare la sicurezza del patrimonio fisico, logico ed informativo dell'azienda.

Tempi di conservazione
All'interno del sistema informatico che gestisce la registrazione delle presenze dei dipendenti i dati vengono conservanti seguendo i criteri ed i tempi di conservazione degli altri dati personali dei dipendenti.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi

Allegato 3

Registro dei trattamenti IRSAP

I dati personali derivanti dal sistema di registrazione delle presenze sono trattati dal solo personale interessato dal trattamento. Potrebbero essere comunicati alle Autorità nei casi previsti da leggi e regolamenti nazionali ed internazionali.	
Individuazione dei contitolari e dei responsabili del trattamento	Nessuno
I dati personali non saranno trasferiti verso Paesi extra UE.	

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	Essendo il trattamento in oggetto gestito dal sistema informatico interno segue le stesse valutazioni indicate per lo stesso. Si rinvia all'analisi del rischio informatico redatta a seguito di consulenza esterna.
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio MEDIO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo (si intende il badge)	_____	_____
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	_____	_____
Danneggiamento dati conservati in cartaceo (si intende il badge)	_____	_____
Danneggiamento dati conservati in digitale	_____	_____
Indisponibilità dei dati conservati in cartaceo (si intende il badge)	_____	_____

Registro dei trattamenti IRSAP

Indisponibilità dei dati conservati in digitale	_____	_____

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "J)" GESTIONE RECLAMI E INFORMAZIONI

Funzione aziendale che svolge il trattamento	L'ufficio Sistema Qualità, e il personale debitamente autorizzato come indicato nell'organigramma
Categoria degli interessati	_____

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- Nome e cognome, - Indirizzo mail - Numero di telefono		

Mezzi di trattamento
I dati personali vengono trattati in formato elettronico

Base giuridica dei dati trattati
- Legittimo interesse del datore (art. 6, par. 1, lett. f del GDPR); - consenso esplicito
. Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di garantire ai propri consumatori ogni supporto e assistenza attinente ai prodotti. Il tempo di conservazione si giustifica al fine di salvaguardare anche sotto gli aspetti della difesa di un diritto in giudizio

Tempi di conservazione
I dati personali saranno conservati per tutta la durata del processo che gestirà il reclamo e per ulteriori dieci anni in ottemperanza ai termini di prescrizione civile. Nel caso dovessero essere comunicati dati particolari questi sono conservati con particolari cautele.

Allegato 3

Registro dei trattamenti IRSAP

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
Nell'ambito del processo di gestione reclami i dati personali non sono comunicati a soggetti terzi rispetto al personale autorizzato. Potrebbero essere comunicati alle Autorità nei casi previsti da leggi e regolamenti nazionali ed internazionali.	
Individuazione dei contitolari e dei responsabili del trattamento	Nessuno
I dati personali non saranno trasferiti verso Paesi extra UE.	

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	Essendo il trattamento in oggetto gestito dal sistema informatico interno segue le stesse valutazioni indicate per lo stesso. Si rinvia all'analisi del rischio informatico redatta a seguito di consulenza esterna .
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio MEDIO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue.	

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo (si intende il badge)	_____	_____
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	_____	_____
Danneggiamento dati conservati in cartaceo (si intende il badge)	_____	_____
Danneggiamento dati conservati in digitale	_____	_____

Registro dei trattamenti IRSAP

Indisponibilità dei dati conservati in cartaceo (si intende il badge)	_____	_____
Indisponibilità dei dati conservati in digitale	_____	_____

SPECIFICHE RELATIVE AL TRATTAMENTO DI CUI ALLA LETTERA "L)" GESTIONE RESPONSABILI E CONTITOLARI DEL TRATTAMENTO

Funzione aziendale che svolge il trattamento	Il relativo ufficio interno di riferimento della ed il consulente esterno come indicato nell'organigramma
Categoria degli interessati	Responsabili e contitolari del trattamento

Categoria dei dati trattati		
Comuni	**Sensibili**	**Giudiziari**
- I dati personali relativi alla gestione del rapporto di lavoro di cui al trattamento "B" - I dati personali relativi alla gestione dei rapporti commerciali di cui ai trattamenti "E", "F" e "G" - I dati relativi al trattamento dei dati per l'attività di promozione "K"	- I dati personali relativi alla gestione del rapporto di lavoro di cui al trattamento "B"; - I dati particolari eventualmente necessari a difendere un diritto in giudizio.	

Mezzi di trattamento
I dati personali vengono trattati sia in formato elettronico che cartaceo

Base giuridica dei dati trattati
- Regolamento UE 679/2016 - Codice Privacy;

Allegato 3

Registro dei trattamenti IRSAP

- Provvedimenti del Garante in materia di gestione dei rapporti di lavoro privati - Autorizzazione generale del Garante n. 1/2016 - Legittimo interesse (art. 6, par. 1, lett. f del GDPR) - Contratto o altro atto giuridico contenente gli obblighi del Responsabile in materia di trattamento dati.
Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f) del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte di di gestire ed organizzare il lavoro aziendale nonché di tutelare la sicurezza del patrimonio fisico, logico ed informativo dell'azienda.

Tempi di conservazione
I tempi di conservazione seguono quelli dei relativi trattamenti richiamati o, nei casi di giudizi, verranno conservati per dieci anni a decorrere dal passaggio in giudicato della sentenza.

Comunicazione dei dati personali, destinatari e trasferimento in Paesi Terzi	
I dati personali sono comunicati secondo i criteri dei rispettivi trattamenti di riferimento. Potrebbero essere comunicati alle Autorità nei casi previsti da leggi e regolamenti nazionali ed internazionali.	
Individuazione dei contitolari e dei responsabili del trattamento	I consulenti esterni sono trattati come responsabili del trattamento ovvero come titolari autonomi del trattamento a seconda della specificità del rapporto commerciale.
I dati personali non saranno trasferiti verso Paesi extra UE.	

MISURE DI SICUREZZA ADOTTATE	
Analisi del rischio in relazione alla tipologia di dati trattati, ai mezzi di trattamento e alle finalità del trattamento	Essendo il trattamento in oggetto gestito dal sistema informatico interno segue le stesse valutazioni indicate per lo stesso. Si rinvia all'analisi del rischio informatico redatta a seguito di consulenza esterna . Sussistono accordi e, eventualmente, nomine che disciplinano specifici impegni e responsabilità volti a trattare adeguatamente i dati personali nel pieno rispetto della normativa vigente.
Sintesi dell'analisi del rischio	
Dalle risultanze dell'analisi del rischio eseguita ne è conseguito che, in considerazione della tipologia di dati trattati, degli archivi utilizzati e delle misure di sicurezza adottate, il Titolare deve tener conto di un rischio MEDIO in relazione ai criteri di Riservatezza, Integrità e Disponibilità posti alla base delle prescrizioni del Regolamento 679/2016 in particolare espresse all'art. 32, così come sintetizzati dalla tabella che segue.	

Allegato 3

Registro dei trattamenti IRSAP

Si allega altresì il rapporto di un'analisi del rischio generale basata sui controlli indicati dalla norma internazionale ISO 27001:2013 (All. J).

Minaccia rispetto ai parametri di Riservatezza, Integrità, Disponibilità	Misura di sicurezza	Analisi
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in cartaceo	_____	_____
Perdita, sottrazione, divulgazione, alterazione, accesso dei dati conservati in digitale	_____	_____
Danneggiamento dati conservati in cartaceo	_____	_____
Danneggiamento dati conservati in digitale	_____	_____
Indisponibilità dei dati conservati in cartaceo	_____	_____
Indisponibilità dei dati conservati in digitale	_____	_____

Allegato 3

Registro dei trattamenti IRSAP

INDICE DELLA DOCUMENTAZIONE ALLEGATA AL REGISTRO DEI TRATTAMENTI

ALLEGATO 1: Asset inventory degli strumenti analogici, elettronici e telematici del Titolare;

ALLEGATO 2: Organigramma Privacy;

ALLEGATO 3: Relazione informatica di analisi del rischio informatico;

ALLEGATO 4: Registro violazioni dei dati personali

ECC….

Allegato 4

REGISTRO DELLE VIOLAZIONI

Nr	Rif. Interno	Dettagli della violazione dati						Misure di sicurezza adottate o da adottare				Procedura
		Data della violazione	Area Processo interessato dalla violazione	Tipologia e numero di interessati coinvolti	Tipologia e volume dati personali coinvolti	Descrizione sintetica della violazione	Responsabili o titolari del trattamento coinvolti	Conseguenze della violazione	Contromisure adottate	Presupposti per notifica al Garante	Presupposti per notifica agli interessati	Verifica e conclusione della procedura

Allegato 5

Data	Registrante	Evento	Conseguenze/effetti	Note	Data aggiornamento	Note aggiornamento

ALLEGATO 6

Gentile …

La informiamo che in data … siamo venuti a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

Presumiamo che in data …, ore …, una terza parte non autorizzata abbiamo acquisito i seguenti dati personali relativi alla Sua posizione:

- …

- …

Le possibili conseguenze dell'evento sono…

In risposta all'evento, abbiamo adottato le seguenti misure di sicurezza:

- …

- …

Per maggiore garanzia, La invitiamo a:

- …

- …

Per qualsiasi informazione o chiarimento, può contattare <Nome Cognome>, <funzione>, ai seguenti recapiti:

- Tel…

- Email…

Si allega scheda informativa della violazione accertata.

Allegato 7

INFORMAZIONI DI SINTESI SULLA VIOLAZIONE

Tempistiche	
Quando è avvenuta la violazione	
Momento in cui il titolare del trattamento è venuto a conoscenza della violazione	
Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione	
Se e/o per quanto tempo la violazione ha comportato l'interruzione del servizio	
Quando il servizio è tornato a funzionare pienamente	

Descrizione della violazione	
Natura della violazione. Perdita integrità, confidenzialità e disponibilità	
Causa della violazione: • Azione interna o esterna intenzionale; • azione interna o esterna accidentale; • azione sconosciuta	

Oggetto della violazione	
Categorie di dati personali (Anagrafici, contatti, credenziali accesso, fiscali, sanitarie, ecc.)	
Volume di dati personali oggetto della violazione	
Categorie di interessati persone fisiche (dipendenti, clienti, contraenti, ecc)	
Volume di interessati coinvolti	

Possibili conseguenze e gravità della violazione	
In caso di perdita di confidenzialità (conseguenze e gravità)	
In caso di perdita di integrità (conseguenze e gravità)	
In caso di perdita di disponibilità (conseguenze e gravità)	

In base alle risposte precedenti che tipo di danni potrebbero aver subito gli interessati?	

Misure adottate a seguito della violazione	
Misure tecniche adottate per porre rimedio alla violazione	
Misure organizzative adottate per porre rimedio alla violazione	
Misure tecniche adottate per ridurre gli effetti negativi per gli interessati	
Misure organizzative adottate per ridurre gli effetti negativi per gli interessati	

irsap
ISTITUTO REGIONALE PER LO SVILUPPO DELLE ATTIVITA' PRODUTTIVE
Ente Pubblico non Economico
L.R. 8/12

Allegato 8

#innovazionenellatrasparenzaperiservizialleimprese

Prot. n. ____ del _____

OGGETTO: Adeguamento Regolamento Europeo GDPR 679/2016 e nuovo Codice della Privacy. - Direttiva sull'utilizzo di spazi di conservazione cloud e reti intranet.

Ai Dirigenti delle Aree e degli Uffici periferici

A tutto il personale

e p.c. Al Commissario ad acta
dott. Giovanni Perino

Al R.P.D.

Premesso che, ai fini della presente direttiva, si richiamano:

- Il codice di comportamento adottato dall'Ente con deliberazione del Consiglio di Amministrazione dell'IRSAP n.4 del 27 febbraio 2014;
- Il D.P.R. 10 gennaio 1957, n. 3 "Testo unico delle disposizioni concernenti lo statuto degli impiegati civili dello Stato", con particolare riferimento all'art. 15 (Segreto d'ufficio) così come novellato dall'art. 28 della L. 7 agosto 1990, n. 241, secondo cui: "L'impiegato deve mantenere il segreto d'ufficio. Non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso. Nell'ambito delle proprie attribuzioni, l'impiegato preposto ad un ufficio rilascia copie ed estratti di atti e documenti di ufficio nei casi non vietati dall'ordinamento";
- Il D.lgs. 33 del 2013 e ss.mm.ii.;

Con riferimento all'oggetto,
preso atto di criticità rilevate nel trattamento e nella conservazione di tali dati, nonché della necessità di adeguarsi oltre al Regolamento 679/2016 anche alle indicazioni tecniche indicate da AGID (in particolare anche con riferimento alla Circolare 18 aprile 2017, n. 2/2017 «Misure minime di sicurezza ICT per le pubbliche amministrazioni);
al fine di garantire, nelle more dell'attivazione di spazi di archiviazione istituzionalizzati, la riservatezza dei documenti di ufficio e dei relativi dati contenuti;
considerato, altresì, che questo Istituto provvederà a breve all'adozione delle specifiche istruzioni in merito alla corretta gestione di tutti gli strumenti informatici dell'Ente da parte dei dipendenti;
con la presente si dispone quanto segue:

Utilizzo degli spazi cloud per archiviazione dati inerenti l'attività lavorativa:
Si chiarisce, in via preliminare, che:

- per cloud (o spazio cloud) si intende la possibilità di archiviazione e gestione di file su spazi di memoria messi a disposizione su internet e più in generale su una rete telematica, comunque esterni al computer dell'utilizzatore;
- per condivisione del cloud si intende la possibilità di accesso all'intero spazio cloud da parte di più soggetti, sia la possibilità di accedere (anche tramite specifico link ipertestuale) ad uno o più determinati file;
- non potranno mai essere ammessi e/o autorizzabili spazi cloud ad uno promiscuo e/o personale;
- lo spazio cloud privato esterno alla rete informatica dell'Ente, eventualmente autorizzato nei termini che seguono, dovrà essere esclusivamente utilizzato per l'attività lavorativa;
- La sicurezza dei dati (in particolare quelli personali) e delle password è obbligo direttamente derivante dall'art. 32 del Reg. UE 679/2016.

Potranno essere utilizzati dai dipendenti solo spazi cloud debitamente autorizzati dalla Direzione Generale.
Tutti gli spazi cloud privati allo stato attualmente utilizzati dovranno essere pertanto oggetto di richiesta di autorizzazione da parte del Dirigente responsabile dell'Ufficio/Area di riferimento.
La predetta autorizzazione dovrà essere richiesta nel più breve tempo possibile e comunque entro e non oltre dieci giorni dall'emanazione e comunicazione della presente direttiva.
In mancanza di richiesta o di negazione dell'autorizzazione è fatto divieto al dipendente di ricorrere all'utilizzo di spazi cloud privati e, in caso di attuale utilizzo, il dipendente dovrà eliminare i dati inseriti nello spazio cloud privato dopo averli trasferiti sul computer in dotazione.
Al fine dell'utilizzazione di tali spazi cloud privati, gli stessi, al momento della richiesta di autorizzazione, dovranno essere dotati di credenziali di accesso e di password che il dirigente dovrà poi fornire, in modalità sicure, solo ed esclusivamente ai dipendenti addetti.
Il Dirigente e i dipendenti saranno responsabili della custodia e della protezione dei dati contenuti nei documenti conservati e condivisi, nonché delle credenziali di accesso in relazione alle quali vige il divieto di trasmetterle a terzi o altri dipendenti non addetti.
È fatto altresì espresso divieto al Dirigente ed al personale autorizzati nei termini predetti di condividere il cloud se non previo espresso provvedimento del superiore gerarchico.
Il Dirigente e i dipendenti avranno l'obbligo di rispettare la riservatezza (diffusione ristretta, riservata o segreta) di tutte le informazioni ivi contenute e ciò in particolare nel caso in cui detti dati dovessero essere personali, di categorie particolari e/o giudiziari così come definiti dal Regolamento Europeo n. 679/2016
In ogni caso, tutti i dati dovranno essere ben organizzati e dovranno essere conservati nei detti spazi di archiviazione autorizzati in cartelle separate e non accessibili in alcun modo dall'esterno.

Reti intranet periferiche

Per le reti intranet locali esistenti, si raccomanda che l'accessibilità debba avvenire solo con credenziali ed in particolar modo le singole cartelle presenti sul server dovranno essere rese accessibili solo al personale di competenza e non visibile al personale di altra Area/Servizio. Tale protezione dei dati dovrà essere oggetto di particolare attenzione per i documenti contenenti dati personali, di categorie particolari e/o giudiziari, nonché per i documenti aventi diffusione riservata.

Si raccomanda la scrupolosa osservanza delle disposizioni sopra riportate.

Il Dirigente dell'Area controllo interno di gestione e anticorruzione
avv. Dario Castrovinci

Il Direttore Generale
ing. Gaetano Collura

Allegato 9

irsap
ISTITUTO REGIONALE PER LO SVILUPPO DELLE ATTIVITA' PRODUTTIVE
Ente Pubblico non Economico
L.R. 8/12

SCHEDA CENSIMENTO AZIENDA

Denominazione sociale:

_____

Nominativo Rappresentante Legale

_____

Indirizzo:

_____

C.A.P.

_____

CITTA'

_____

Sede legale (indirizzo se diverso dalla sede azienda)

_____

Codice fiscale:

_____

Partita IVA:

_____

Forma giuridica:

1	Impresa individuale	☐
2	Società di persone	☐
3	Società di capitali	☐

_____

E-mail :

_____

SCHEDA CENSIMENTO AZIENDA

Indirizzo PEC:

_____

Telefono:

_____

Sito internet:

_____

Numero REA:

_____

Attività:

_____

Stato attività insediamento:

Attiva	☐
Non attiva	☐
In fase di insediamento	☐

Settore di appartenenza e prodotti

1	Industria	☐
2	Artigianato	☐
3	Commercio	☐
4	Servizi	☐
5	Agricoltura	☐

Altro: _____

ELENCO BENI E SERVIZI PRODOTTI

Classificazione ATECO:

_____

SCHEDA CENSIMENTO AZIENDA

_____

_____

_____

_____

Anno di costituzione:

_____

Dipendenti

Tipologia	N.
A tempo indeterminato	
A tempo determinato	

Fatturato:

classe di fatturato	
da 50.000 a 100.00	☐
da 100.001 a 250.000	☐
da 250.001 a 500.000	☐
da 500.001 a 1.000.000	☐
da 1.000.001 a 2.000.000	☐
Oltre 2.000.000	☐

ANNOTAZIONI:

_____

_____

_____

_____

_____

SCHEDA CENSIMENTO AZIENDA

PARTE TECNICA

Area Industriale di insediamento:

_____

Lotto:

_____

Superfice complessiva del lotto

_____

Estremi catastali:

Sezione censuaria:

Terreno	☐
Fabbricati	☐

territorio di

Foglio:

_____

Particelle:

_____

_____

_____

_____

_____

Assegnazione:

Estremi assegnazione: _____

Stato assegnazione: _____

SCHEDA CENSIMENTO AZIENDA

Note: _____

_____

_____

_____

Provvedimenti urbanistici di autorizzazione:

Concessione edilizia:
_____

Agibilità:
_____

Autorizzazione Unica Ambientale:

autorizzazione agli scarichi di acque reflue di cui al capo II del titolo IV della sezione II della Parte terza del decreto legislativo 3 aprile 2006, n. 152 e successive modificazioni (di seguito Codice dell'ambiente)	☐
comunicazione o nulla osta relativi all'impatto acustico di cui all'articolo 8, commi 4 o comma 6, della legge 26 ottobre 1995, n. 447;	☐
autorizzazione all'utilizzo dei fanghi derivanti dal processo di depurazione in agricoltura di cui all'articolo 9 del decreto legislativo 27 gennaio 1992, n. 99	☐
comunicazioni relative alle operazioni di smaltimento e recupero di rifiuti di cui agli articoli 215 e 216 del Codice dell'ambiente	☐
altri atti di comunicazione, notifica ed autorizzazione in materia ambientale compresi nell'AUA in base alla normativa regionale (specificare) _____	☐

ANNOTAZIONI:

_____

_____

_____

_____

_____

SCHEDA CENSIMENTO AZIENDA

Istituto Regionale per lo Sviluppo delle Attività Produttive
Informativa completa sul trattamento dei dati personali per censimento imprese

N° Rev.	Data Emissione/Revisione	Descrizione	Firma Responsabile Interno
00	_____	Prima Emissione	

Il Regolamento Europeo 679/2016 (di seguito anche "Regolamento" e/o "GDPR") disciplina la tutela delle persone fisiche con riguardo al trattamento dei dati personali nel rispetto dei principi di correttezza, liceità, nonché per la salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento.

Il presente documento esplicativo si deve ritenere parte integrante dell'informativa semplificata comunicata e sottoscritta al momento della ricezione del questionario, ovvero in occasione di modifiche e/o aggiornamenti della stessa dovuti a scelte dell'Ente e/o obblighi normativi.
Il documento riporta in maniera dettagliata e maggiormente approfondita le indicazioni obbligatorie previste dall'art. 13 ("Informazioni da fornire qualora i dati personali siano raccolti presso l'Interessato").

In calce all'informativa sono riportati integralmente i seguenti articoli del GDPR:

1) art. 4, "Definizioni";
2) art. 5 "Liceità del trattamento";
3) art. 12 "Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'Interessato";
4) art. 15 "Diritto di accesso dell'Interessato";
5) art. 16 "Diritto di rettifica";
6) art. 17 "Diritto alla cancellazione; c.d. diritto all'oblio";
7) art. 18 "Diritto di limitazione di trattamento";
8) art. 20 "Diritto alla portabilità dei dati";
9) art. 21 "Diritto di opposizione";
10) art. 22 "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"
11) art. 77 "Diritto di proporre reclamo all'autorità di controllo";
12) art. 78 "Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo";
13) art. 79 "Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento";
14) art. 82 "Diritto al risarcimento e responsabilità"

1. Titolare del trattamento

1.1 Il Titolare del trattamento dei dati personali è l'Istituto Regionale per lo Sviluppo delle Attività Produttive (di seguito anche soltanto "Titolare" e/o "IRSAP" e/o "Ente"), p. i.v.a. 06141650827 e c.f. 97279190827, n. iscr. al Registro Imprese PA - 312065, Codice IPA: UF8748, con rappresentante legale Perino Giovanni nella qualità di Commissario Straordinario.

1.2 Il Titolare del trattamento può essere contattato presso:

a) la sede legale in via Enrico Ferruzza Sud Ovest n. 1/5, Palermo CAP 90124;
b) al numero 091/77287;
c) all'indirizzo mail ordinaria info@irsapsicilia.it;
d) all'indirizzo pec info@pec.irsapsicilia.it.

1.3 Il Titolare indica quale Responsabile della Protezione Dati il _____ _____ che può essere contattato a _____.

1.4. Per l'esercizio dei diritti IRSAP ha predeterminato le apposite procedure di gestione. Le modalità di esercizio dei diritti verranno comunicate all'Interessato a seguito di ogni legittima richiesta del medesimo ad uno dei contatti sopra elencati.

2. Finalità del trattamento

2.1 I dati personali sono raccolti al fine di eseguire un censimento delle imprese del territorio siciliano nell'ambito del quale IRSAP svolge le proprie funzioni pubbliche istituzionali.
2.3 Per il perseguimento delle predette finalità fornire le informazioni richieste è facoltativo. In caso di mancata o errata comunicazione l'Ente potrebbe on essere in grado di fornire i servizi di cui al proprio Statuto. Nell'ipotesi in cui i dati si fornissero inesatti o falsi potrebbero conseguire responsabilità civile e/o penali.
2.4 L'IRSAP non tratta dati genetici neppure con il consenso dell'interessato.

3. Dettaglio dati trattati, base giuridica del trattamento e periodo di conservazione.

3.1. La tabella che segue riporta un elenco dei dati trattati dal Titolare sulla base delle informazioni fornite direttamente dall'Interessato, nonché la base giuridica (cioè la giustificazione legale del trattamento) e il periodo di conservazione.

Tipologia di dati personali		Base giuridica del trattamento	Periodo di conservazione del trattamento
Dati personali comuni	- Dati anagrafici dei legali rappresentanti delle imprese; - Residenza dei legali rappresentanti delle imprese - Codice fiscale dei legali rappresentanti delle imprese; - Contatti dei legali rappresentanti delle imprese .	- L. R. Sicilia 8/2012; - Statuto IRSAP e succ. mod. - Reg. UE 679/2016, art. 5, comma 1, lett. e), comma e, lett. b); - D.Lgs 196/2003, artt. 2-ter, 59, 61, Titolo VII (Capi I e II) - Legittimo interesse del datore (art. 6, par. 1, lett. f del GDPR);	I dati vengono pubblicati per un periodo di cinque anni. Successivamente potranno essere archiviati e conservati (non pubblicati) ai sensi di legge ai fini del perseguimento del pubblico interesse.
Dati di categorie particolari	Non vengono trattati dati di		
Dati giudiziari	Non vengono trattati dati giudiziari		

3.2. Il trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f del Regolamento, relativo ai legittimi interessi perseguiti dal Titolare, si fonda sulla necessità da parte dell'IRSAP in particolare di verificare e valutare le tempistiche, le modalità ed i limiti di archiviazione nel pubblico interesse così come previsto dall'art. 99 del D.lgs 196/2003, nonché per difendere un proprio diritto in giudizio in caso di contestazioni.

4. Processi decisionali automatizzati, compresa la profilazione

4.1 Per nessuna delle finalità di cui alla presente informativa, il trattamento dei dati personali e particolari degli interessati, da parte di IRSAP, non prevede l'esistenza di processi decisionali automatizzati (cioè scelte determinati in assenza di un intervento umano), compresa la profilazione (cioè l'individuazione delle abitudini di una persona fisica), che possano comportare effetti giuridici che riguardano gli interessati o che incidano sugli stessi in modo rilevante.

5. Comunicazione dei dati personali e destinatari

5.1 I dati personali saranno comunicati, in stretta relazione alle finalità sopra indicate, quei dipendenti dell'IRSAP espressamente autorizzati al trattamento ed in particolare:

- I dirigenti degli istituti periferici;
- I responsabili del procedimento espressamente nominati;
- L'area programmazione strategica.
- La direzione centrale IRSAP
- Le Società terze, nominate responsabili del trattamento, al fine della pubblicazione dei dati raccolti sul sito istituzionale di IRSAP (www.irsapsicilia.it) e della gestione tecnica dello stesso.

5.2 I dati non saranno trasferiti verso Paesi extra UE. In caso di trasferimento di dati verso Paesi terzi, Elle Costruzioni provvederà a comunicarlo debitamente fornendo le idonee informative ai sensi dell'art. 13, 1° comma, lett. "f)" e, ove necessario, richiedendo il necessario consenso.

I DIRITTI DELL'INTERESSATO

6. Diritto di revoca del consenso

6.1 Nei casi in cui il trattamento è fondato sul consenso l'Interessato, sussistendo i presupposti di legge, ha il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca

7. Diritto di accesso

7.1 L'Interessato potrà chiedere al Titolare:

a) la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
b) l'accesso ai propri dati personali elencanti agli artt. 12 e 15 riportati in calce.

7.2 Il presente diritto è gratuito salve le eccezioni previste dal Regolamento.

7.3 Il ricorso al diritto di accesso non può ledere i diritti e le libertà altrui.

8. Diritto di rettifica o integrazione

8.1 L'Interessato ha il diritto di ottenere dal Titolare la rettifica dei dati personali inesatti e, tenuto conto delle finalità del trattamento, ha il diritto di ottenere l'integrazione dei dati personali incompleti.

8.2 I diritti di accesso o rettifica sono disciplinati agli artt. 12, 15 e 19 riportati in calce.

9. Diritto alla cancellazione

9.1 L'Interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali se sussiste uno degli specifici motivi previsti all'art. 16 riportato in calce.

9.2 L'Interessato potrà chiedere la cancellazione dei propri dati personali secondo le modalità previste agli artt. 12, 16 e 19 riportati in calce.

10. Diritto alla limitazione del trattamento

10.1 L'Interessato ha il diritto che i propri dati personali non siano ulteriormente trattati, ma non cancellati se sussiste uno degli specifici motivi previsti all'art. 17 riportato in calce.

10.2 Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato, salvi i casi di: consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante.

10.3 L'Interessato potrà chiedere la cancellazione dei propri dati personali secondo le modalità previste agli artt. 12, 17 e 19 riportati in calce.

11. Diritto di opposizione

11.1 L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione.
11.2 L'Interessato potrà far valere il diritto di opposizione sulla base dei presupposti e nelle modalità previste all'art. 21 riportato in calce.

12. Diritto alla portabilità
12.1 L'Interessato ha il diritto di ricevere dati personali, in un formato strutturato, di uso comune e leggibile meccanicamente.
12.2 L'Interessato ha il diritto di memorizzar i dati personali su un dispositivo nella propria disponibilità per fini personali, senza trasferirli a un diverso titolare.
12.3 L'Interessato ha il diritto di trasmettere i propri dati personali da un titolare del trattamento a un altro senza impedimenti.
12.4 Il diritto alla portabilità potrà essere fatto valere nei termini e nei limiti stabiliti all'art. 20 riportato in calce.

13. Diritto di proporre reclamo
13.1 Al fine di far valere i propri diritti l'Interessato potrà rivolgersi, nelle modalità e nei termini previsti dagli artt. 77, 78, 79 e 82 riportati in calce, all'Autorità Giudiziaria oppure al Garante per la protezione dei dati di cui si riportano qui di seguito i recapiti:

- Piazza Venezia n. 11 - 00187 Roma;
- Fax: (+39) 06.69677.3785 - Centralino telefonico: (+39) 06.696771;
- E-mail: garante@gpdp.it - Posta certificata: protocollo@pec.gpdp.it.

ARTICOLI DEL REGOLAMENTO RICHIAMATI NELL'INFORMATIVA

Articolo 4 Definizioni

Ai fini del presente regolamento s'intende per:

1) **«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 a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) **«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, come 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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) **«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;
5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a 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;
6) **«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;
7) **«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) **«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;
9) **«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. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10) **«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;

11) **«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, che i dati personali che lo riguardano siano oggetto di trattamento;
12) **«violazione dei dati personali»**: 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;
13) **«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;
14) **«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;
15) **«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;
16) **«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 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 presente regolamento;
17) **«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, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
18) **«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;
19) **«gruppo imprenditoriale»**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20) **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
21) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22) **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati

in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) **«trattamento transfrontaliero»**: a) 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 b) 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;
24) **«obiezione pertinente e motivata»**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25) **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);
26) **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 5 Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
   a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
   b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
   d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
   e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
   f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
   a) dal diritto dell'Unione; o
   b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico

interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; d
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 12 Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'Interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'Interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'Interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'Interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'Interessato.

3. Il titolare del trattamento fornisce all'Interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'Interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'Interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato.

4. Se non ottempera alla richiesta dell'Interessato, il titolare del trattamento informa l'Interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi

dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'Interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'Interessato.
7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Articolo 15 Diritto di accesso dell'Interessato
1. L'Interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'Interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.
3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'Interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'Interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Articolo 16 Diritto di rettifica
L'Interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 17 Diritto alla cancellazione ("diritto all'oblio")
1. L'Interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'Interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'Interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'Interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 18 Diritto di limitazione di trattamento
1. L'Interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
a) l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono 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 ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'Interessato.
2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
3. L'Interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Articolo 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'Interessato tali destinatari qualora l'Interessato lo richieda.

Articolo 20 Diritto alla portabilità dei dati

1. L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Articolo 21 Diritto di opposizione

1. L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. 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.
3. Qualora l'Interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'Interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'Interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'Interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6.Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'Interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato;
c) si basi sul consenso esplicito dell'Interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'Interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato.

Articolo 77 Diritto di proporre reclamo all'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'Interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.
2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Articolo 78 Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.
2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun Interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.
3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

Articolo 79 Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni Interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.
2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'Interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Articolo 82 Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'Interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.
6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Questo documento spiega come IRSAP utilizza i dati personali
LEGGERE ATTENTAMENTE

Il **dato personale** è l'informazione (es.: nome, numero identificativo, dati anche on line sull'identità personale, economica, o sociale) che identifica, anche indirettamente, o potrebbe identificare una persona fisica.

Questo è un documento riassuntivo. È possibile chiedere l'informativa completa via mail (info@irsapsicilia.it) o direttamente all'URP dell'ufficio centrale o periferico di riferimento.
È possibile chiedere chiarimenti al Responsabile Protezione dati all'indirizzo _____

Chi tratta i dati	**I.R.S.A.P.,** via E. Ferruzza Sud/Ovest 1/5, 90124 Palermo
Quali dati personali vengono trattati	Dati anagrafici, residenza, codice fiscale e contatti del legale rappresentante dell'impresa (società di capitali, società di persone e/o ditta individuale):
Le finalità e la giustificazione legale del trattamento	Al fine del perseguimento dei propri fini istituzionali e statutari l'IRSAP (pubblicati su www.irsapsicilia.it), quale ente pubblico non economico, deve procedere al censimento delle aziende del territorio siciliano
Obbligo di fornire i dati.	Comunicare i dati è facoltativo. Se non si forniscono o si forniscono errati l'IRSAP potrebbe non essere in grado di erogare i servizi; se si comunicano inesatti o falsi potrebbero conseguirne responsabilità civili e penali.
A chi possono essere comunicati i dati	Tutti i dati personali saranno comunicati ai dipendenti IRSAP debitamente istruiti, nonché ai soggetti autorizzati ad accedervi per legge. Vi potrebbero accedere i fornitori dei servizi esterni per ragioni di manutenzione e aggiornamento dei sistemi informatici I dati personali non verranno trasferiti fuori dall'Europa od a organizzazioni internazionali. I dati personali non vengono diffusi.
Strumenti di gestione dati e sicurezza	Per la gestione di tutti i dati saranno utilizzati sia strumenti cartacei che informatici. Tutti gli strumenti sono sottoposti ad attente misure di sicurezza e tutela.
Tempo di conservazione	Tutti i dati saranno pubblicati per cinque anni. Potranno essere ulteriormente conservati a fini di archiviazione nell'interesse pubblico.

I DIRITTI

A seguito di una richiesta via posta ordinaria o mail (utilizzando i recapiti su indicati o quelli nell'informativa completa), via pec o anche oralmente, vengono garantiti i seguenti diritti:

- **a)** accedere e/o chiedere se IRSAP è in possesso di dati personali;
- **b)** far correggere i dati personali;
- **c)** bloccare, limitare od opporsi all'uso dei dati personali;
- **d)** far cancellare i dati personali,
- **e)** farsi dare i dati anche per trasferirli ad altro Titolare.

Per i propri diritti è possibile rivolgersi al Garante dei Dati Personali o all'Autorità Giudiziaria.

IRSAP assicura che i dati personali vengono utilizzati solo per quel che c'è scritto in questo documento e se ci fosse la necessità di utilizzarli per altri scopi lo comunicherà, fornendo ogni idonea informativa e, se del caso, chiedendo prima ogni necessario consenso.

Luogo e data,_____ Timbro e firma per presa visione.

Allegato 12

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

degli utenti che consultano i siti web dell'Istituto Regionale per lo sviluppo delle Attività Produttive (IRSAP), Ente Pubblico non economico L.R. 8/2012, ai sensi dell'articolo 13 del Regolamento (UE) 2016/679

PERCHÉ QUESTE INFORMAZIONI

Ai sensi del Regolamento (UE) 2016/679 (di seguito "Regolamento"), questa pagina descrive le modalità di trattamento dei dati personali degli utenti che consultano i siti web di IRSAP accessibili per via telematica ai seguenti indirizzi:

1. www.irsapsicilia.it/;
2. http://cloud.urbi.it/urbi/progs/urp/solhome.sto?DB_NAME=n1200384&areaAttiva=1.

Le presenti informazioni non riguardano altri siti, pagine o servizi online raggiungibili tramite link ipertestuali eventualmente pubblicati nei siti ma riferiti a risorse esterne al dominio di IRSAP.

TITOLARE DEL TRATTAMENTO

A seguito della consultazione dei siti sopra elencati possono essere trattati dati relativi a persone fisiche identificate o identificabili.

Titolare del trattamento è l'Istituto Regionale per lo Sviluppo delle Attività Produttive (di seguito anche soltanto "Titolare" e/o "IRSAP" e/o "Ente"), p. i.v.a. 06141650827 e c.f. 97279190827, n. iscr. al Registro Imprese PA - 312065, Codice IPA: UF8748, con rappresentante legale Perino Giovanni nella qualità di Commissario Straordinario.

Il Titolare del trattamento può essere contattato presso:

a) la sede legale in via Enrico Ferruzza Sud Ovest n. 1/5, Palermo CAP 90124;
b) al numero 091/77287;
c) all'indirizzo mail ordinaria info@irsapsicilia.it;
d) all'indirizzo pec info@pec.irsapsicilia.it.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della Protezione dei Dati (RPD) è raggiungibile al seguente indirizzo: via Enrico Ferruzza Sud Ovest n. 1/5, Palermo CAP 90124, Roma, email: emiliano.v@deas.it.

BASE GIURIDICA DEL TRATTAMENTO

I dati personali indicati in questa pagina sono trattati dall'IRSAP nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri ed istituzionali così come descritti nell'atto costitutivo e nello Statuto facilmente consultabili direttamente dal sito internet.

TIPI DI DATI TRATTATI E FINALITÀ DEL TRATTAMENTO

<u>Dati di navigazione</u>

I sistemi informatici e le procedure software preposte al funzionamento di questo sito acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer e dei terminali utilizzati dagli utenti, gli indirizzi in notazione URI/URL (Uniform Resource Identifier/Locator) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Tali dati, necessari per la fruizione dei servizi web, vengono anche trattati allo scopo di:

- ottenere informazioni statistiche sull'uso dei servizi (pagine più visitate, numero di visitatori per fascia oraria o giornaliera, aree geografiche di provenienza, ecc.);
- controllare il corretto funzionamento dei servizi offerti.

I dati di navigazione non persistono per più di sette giorni (salve eventuali necessità di accertamento di reati da parte dell'Autorità giudiziaria).

Dati comunicati dall'utente

L'invio facoltativo, esplicito e volontario di messaggi agli indirizzi di contatto dell'IRSAP, i messaggi privati inviati dagli utenti ai profili/pagine istituzionali sui social media (laddove questa possibilità sia prevista), nonché la compilazione e l'inoltro dei moduli presenti sui siti dell'Ente, comportano l'acquisizione dei dati di contatto del mittente, necessari a rispondere, nonché di tutti i dati personali inclusi nelle comunicazioni.

Specifiche informative verranno pubblicate nelle pagine dei siti dell'IRSAP predisposte per l'erogazione di determinati servizi.

Cookie e altri sistemi di tracciamento

Non viene fatto uso di cookie per la profilazione degli utenti, né vengono impiegati altri metodi di tracciamento.

Viene invece fatto uso di cookie di sessione (non persistenti) in modo strettamente limitato a quanto necessario per la navigazione sicura ed efficiente dei siti. La memorizzazione dei cookie di sessione nei terminali o nei browser è sotto il controllo dell'utente, laddove sui server, al termine delle sessioni HTTP, informazioni relative ai cookie restano registrate nei log dei servizi, con tempi di conservazione comunque non superiori ai sette giorni al pari degli altri dati di navigazione.

DESTINATARI DEI DATI

Sono destinatari dei dati raccolti a seguito della consultazione dei siti sopra elencati i seguenti soggetti designati dal Garante, ai sensi dell'articolo 28 del Regolamento, quali responsabili del trattamento:

- _____, relativamente al sito www.irsapsicilia.it quale fornitore dei servizi di sviluppo, erogazione e gestione operativa delle piattaforme tecnologiche impiegate;
- PADigitale SPA, relativamente al sito http://cloud.urbi.it/urbi/progs/urp/solhome.sto?DB_NAME=n1200384&areaAttiva=1 quale fornitore dei servizi di sviluppo, erogazione e gestione operativa delle piattaforme tecnologiche impiegate.

I dati personali raccolti sono altresì trattati dal personale dell'IRSAP, che agisce sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento medesimo.

DIRITTI DEGLI INTERESSATI

Gli interessati hanno il diritto di ottenere dall'IRSAP, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati agli indirizzi sopra indicati.

DIRITTO DI RECLAMO

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti effettuato attraverso questo sito avvenga in violazione di quanto previsto dal Regolamento hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

Allegato 13 **Informativa semplificata trattamento dati per emergenza covid-19**

Chi tratta i dati	**IRSAP** Via Ferruzza n. 5- 90124 Palermo. Mail: info@irsapsicilia.it; Tel 091 77287; pec: info@pec.irsapsicilia.it
Contatti RPD	
I dati personali e trattati (anche di categorie particolari)	Nell'attuale contesto emergenziale possono essere trattati i dati: - anagrafici propri e di persone conviventi; - sulla professione, attività lavorativa e luoghi di lavoro; - sulla zona di provenienza e/o transito a rischio; - sul domicilio di isolamento fiduciario; - sulla salute dell'interessato e relativo monitoraggio.
Trattamento per finalità di interesse pubblico	Garantire la protezione dall'emergenza e la sorveglianza sanitaria, nonché assicurare l'assistenza dei contagiati e la gestione dell'attività all'interno dell'azienda. Il trattamento è legittimo in base ai protocolli di sicurezza anti-contagio indicati dalle norme e dai decreti del Governo Italiano vigenti. **Non si procederà alla registrazione della misurazione di temperatura o altri dati, salvo nei casi consentiti dalla legge**
Obbligo di fornire i dati.	Per il dipendente è obbligatorio. Per il visitatore è facoltativo. Se non si forniscono o si comunicano inesatti o falsi, non sarà possibile ammettere l'interessato negli uffici aziendali.
A chi possono essere comunicati i dati	Tutti i dati personali saranno comunicati ai dipendenti debitamente istruiti, se di necessità al medico competente, nonché **ai** soggetti autorizzati ad accedervi per legge. I dati personali e particolari non verranno trasferiti fuori dall'Europa od a organizzazioni internazionali. I dati personali non vengono diffusi.
Strumenti di gestione dati.	Per la gestione di tutti i dati saranno utilizzati sia strumenti cartacei che informatici.
Tempo di conservazione	Tutti i dati saranno conservati sino al termine dello stato d'emergenza.

I DIRITTI

A seguito di una richiesta via posta ordinaria o pec (utilizzando i recapiti su indicati o quelli nell'informativa completa) o oralmente, vengono garantiti i seguenti diritti:

a) accedere e/o chiedere se **IRSAP** è in possesso di dati personali;
b) far correggere i dati personali;
c) bloccare, limitare od opporsi all'uso dei dati personali;
d) far cancellare i dati personali,
e) farsi dare i dati anche per trasferirli ad altro Titolare.

Per far valere i diritti è possibile rivolgersi all'Autorità per la Protezione dei Dati Personali o all'Autorità Giudiziaria.

IRSAP assicura che i dati personali vengono utilizzati solo per quel che c'è scritto in questo documento e se ci fosse la necessità di utilizzarli per altri scopi lo comunicherà, fornendo ogni idonea informativa e, se del caso, chiedendo prima ogni necessario consenso.

Allegato 14

QUESTO DOCUMENTO SPIEGA COME VENGONO UTILIZZATI I TUOI DATI PERSONALI LEGGI ATTENTAMENTE

Il **dato personale** è l'informazione che identifica, anche indirettamente, o potrebbe identificare una persona fisica.
I **dati di categorie particolari**, invece, sono le informazioni sulla tua salute.
I **dati giudiziari**, sono le informazioni relative ali procedimenti ed alle condanne penali.
Questo è un documento sintetico è tuo diritto chiedere quello completo.

Chi tratta i tuoi dati?	**I.R.S.A.P.,** info@irsapsicilia.it, via E. Ferruzza Sud/Ovest 1/5, 90124 Palermo.
Quali dati personali?	Anagrafici, residenza, contatti, dati retributivi, familiari (eventuale), fiscali, immagini (inclusa videosorveglianza se presente), dati informatici (se connessi all'attività lavorativa).
Quali dati particolari o giudiziari?	Ove necessari all'esecuzione rapporto di lavoro ovvero se prescritto dalla legge: i dati sanitari, i dati biometrici, tutti i dati giudiziari.
Per quali finalità e su quali basi avviene il trattamento?	I dati personali servono per gestire il rapporto di lavoro, la Tua salute e sicurezza, il patrimonio e le esigenze organizzative dell'Ente. Li possiamo usare perché: **a)** hai sottoscritto il contratto di lavoro; **b)** hai, eventualmente, sottoscritto un consenso (per trattamenti ulteriori rispetto al contratto); **c)** ci sono delle leggi che ci obbligano a chiederli. Non si cercheranno di capire i tuoi comportamenti o abitudini in modo automatizzato (cioè tramite un computer senza l'intervento umano).
È obbligatorio fornire i dati personali?	Comunicare i dati personali e particolari sopra indicati è obbligatorio. Se non li fornisci oppure li comunichi errati, inesatti o falsi, potrebbero esserci anche responsabilità disciplinari e/o contrattuali. Per gli eventuali trattamenti ulteriori, invece, il consenso è facoltativo.
A chi vengono comunicati i dati?	Secondo specifiche leggi, finalità, nomine, accordi e/o istruzioni: **a)** ai dipendenti e/o ai consulenti (i.e. legali, fiscali, lavoro, sicurezza); **b)** alle Società, Enti Pubblici e/o PP.AA. per il perseguimento di fini istituzionali; **c)** ai soggetti autorizzati a trattarli per disposizione di legge. I dati personali e particolari non verranno trasferiti fuori dall'Europa od a organizzazioni internazionali. I dati personali non vengono diffusi
Come trattiamo i dati?	Per la gestione di tutti i dati saranno utilizzati sia strumenti cartacei che informatici.
Per quanto tempo si conservano i dati?	Per tutta la durata del contratto di lavoro, per ulteriori dieci anni e comunque nei termini di legge.

I DIRITTI

A seguito di una richiesta via posta ordinaria o pec (utilizzando i recapiti su indicati o quelli nell'informativa completa) o oralmente, vengono garantiti i seguenti diritti:

- **a)** accedere e/o chiedere se IRSAP è in possesso di dati personali;
- **b)** far correggere i dati personali;
- **c)** bloccare, limitare od opporsi all'uso dei dati;
- **d)** far cancellare i dati personali,
- **e)** farsi dare i dati per trasferirli ad altro Titolare;
- **f)** chiedere che i tuoi dati siano visualizzati esclusivamente dal tuo medico curante

Per far valere i tuoi diritti puoi rivolgerti al Garante Privacy o all'Autorità Giudiziaria. L'IRSAP assicura che i dati personali vengono utilizzati solo per quanto su indicato e se ci fosse la necessità di utilizzarli per altri scopi te lo comunicherà, fornendo ogni idonea informativa e chiedendo il tuo consenso.

_____, _____

Per ricevuta del dipendente

_____

Allegato 15

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI
PROFESSIONISTI/CONSULENTI/COLLABORATORI ESTERNI

Premessa

Ai sensi dell'art. 13 del D. Lgs. 196/2003 (di seguito "Codice Privacy") e dell'art. 13 del Regolamento UE n. 2016/679 (di seguito "GDPR 2016/679"), recante disposizioni a tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, L' IRSAP con il presente atto informa i collaboratori, i consulenti, i professionisti esterni, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo), sulle modalità di trattamento dei dati personali raccolti.

Con il termine dati personali si fa riferimento alla definizione contenuta nell'articolo 4 al punto 1) del Regolamento ossia "qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Con il termine trattamento di Dati Personali si fa riferimento alla definizione contenuta nell'articolo 4 al punto 2) del Regolamento in base al quale costituisce trattamento dei dati personali "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, come 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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Il Regolamento prevede che, prima di procedere al trattamento di Dati Personali è necessario che la persona a cui tali Dati Personali appartengono sia informata circa i motivi per i quali tali dati sono richiesti ed in che modo verranno utilizzati.

A tal proposito, il presente documento ha lo scopo di fornire, in maniera semplice ed intuitiva, tutte le informazioni utili e necessarie affinché il conferimento dei Dati Personali avvenga in modo consapevole ed informato e, in qualsiasi momento, poter richiedere ed ottenere chiarimenti e/o rettifiche.
La presente informativa, quindi, è redatta sulla base del principio della trasparenza e di tutti gli elementi richiesti dall'articolo 13 del Regolamento ed è articolata in singole sezioni numerate ognuna delle quali riferita ad uno specifico argomento in modo da rendere la lettura più rapida, agevole e di facile comprensione.

1) Titolare del trattamento

I.R.S.A.P., info@irsapsicilia.it, via E. Ferruzza Sud/Ovest 1/5, 90124 Palermo.

2) Responsabile della protezione dei dati (RPD)

L'IRSAP si riserva di comunicare il nominativo del Responsabile per la Protezione dei Dati (RPD).

3) Fonte dei dati e tipologia di dati trattatI

I dati personali possono essere raccolti:
- presso l'interessato (es. all'atto della formalizzazione del rapporto di lavoro o all'atto della richiesta di uno specifico servizio, anche mediante servizi on line);
- presso fonti ad accesso pubblico
- presso soggetti terzi per il perseguimento di scopi istituzionali del'IRSAP

E' possibile che nell'ambito delle attività istituzionali l'IRSAP si trovi a trattare dati personali particolari quali ad esempio quelli sensibili e giudiziari (condizioni economiche disagiate, stato di salute o di disabilità, procedimenti disciplinari, ecc.). In ogni caso i predetti dati saranno trattati esclusivamente per il perseguimento delle finalità istituzionali e nel rispetto della citata normativa e degli obblighi di riservatezza cui è sempre ispirata l'attività dell'Istituto

.

4) Modalità di trattamento e conservazione

Il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità perseguite e, comunque, in modo da garantire la sicurezza e la riservatezza

dei dati stessi nel rispetto di quanto previsto dall'art. 32 del GDPR 2016/679 e dall'Allegato B del D.Lgs. 196/2003 (artt. 33-36 del Codice) in materia di misure di sicurezza, ad opera di soggetti appositamente incaricati e in ottemperanza a quanto previsto dagli art. 29 GDPR 2016/ 679.
L'archiviazione della documentazione è effettuata sia in modalità elettronica che cartacea.
I dati personali sono conservati per il periodo di tempo necessario al conseguimento delle finalità per le quali sono raccolti e trattati o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari a cui l'organizzazione debba attenersi

5) Finalità del trattamento
I dati personali, ivi compresi quelli sensibili e giudiziari, sono trattati nell'ambito della normale attività dell'IRSAP e secondo le finalità istituzionali perseguite come di seguito meglio specificate a solo titolo esemplificativo e non esaustivo:
5.a) Finalità strettamente connesse e strumentali alla gestione del rapporto di lavoro in qualunque forma ed alla gestione/organizzazione di attività tipiche dell'organizzazione (es. inoltro comunicazioni organizzative legate all'attività, organizzazione di sistemi di gestione, erogazione di servizi ritenuti dall'Ente necessari al fine di svolgere in maniera competente la propria attività, comunicazioni della direzione relativamente all'organizzazione e gestione delle attività degli organi dell'Ente, conservazione dei dati per finalità di costituzione di data-base, ecc), comprese le finalità di interesse legittimo correlate ovvero gli adempimenti amministrativi, contabili e fiscali connessi agli obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria, nonché da disposizioni impartite da autorità a ciò legittimate dalla legge e da organi di vigilanza e controllo (ad es. adempimenti contabili, retributivi, previdenziali, assistenziali, fiscali, ecc).
5.b) In riferimento all'eventuale trattamento di dati sensibili e giudiziari le finalità di rilevante interesse pubblico perseguite potrebbero essere le seguenti: instaurazione e gestione di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato; applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
5.c) Gestione di un'eventuale contenzioso giudiziale, stragiudiziale e attività di consulenza.
5.d)Eventuali comunicazioni istituzionali, al fine di perseguire le finalità esplicitate nello Statuto, effettuate tramite materiale testuale/foto/audio/video su mezzi di comunicazione elettronici (ad es. via internet) o tradizionali (es. stampa, news, brouchure, etc) inerenti le attività/iniziative gestite dall'Ente che possono contenere dati ed immagini/video/audio raffiguranti esplicitamente l'interessato
Qualora il titolare intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, esso fornirà previamente all'interessato ogni informazione necessaria.
6) Ambito di comunicazione e diffusione
I dati personali sono conosciuti e trattati, nel rispetto della vigente normativa in materia, dal personale dell'IRSAP, individuato come incaricato del trattamento, in servizio presso le strutture di pertinenza.
I dati personali raccolti dall'IRSAP possono essere comunicati, nei limiti strettamente pertinenti alle finalità suindicate, anche a soggetti o categorie di soggetti (anche all'estero) cui la comunicazione è prevista per legge, per regolamento o dalla normativa nazionale e comunitaria nonché, per l'esecuzione degli obblighi contrattuali o precontrattuali (ad esempio: Pubbliche amministrazioni, Istituti di Credito, Compagnie di Assicurazione, Consulenti e Liberi professionisti legali, contabili, del lavoro, ecc.)
I dati personali raccolti dall'IRSAP possono essere comunicati inoltre a:
- Soggetti cui la comunicazione è prevista per legge, per regolamento o dalla normativa nazionale e comunitaria (ad esempio pubbliche amministrazioni ed enti tra i cui compiti rientrino quelli della tutela e sicurezza nei luoghi di lavoro) nonché, per l'esecuzione degli obblighi contrattuali o precontrattuali (Istituti di Credito, Compagnie di Assicurazione, ecc.);
- Soggetti cui fosse indispensabile comunicare tali dati per le attivita' strettamente legate al rapporto in essere con l'IRSAP, ad esempio consulenti, professionisti,tribunali collaboratori o fornitori che collaborano per aspetti legati alla gestione delle attività
- Consulenti legali, contabili, del lavoro al fine dello studio e risoluzione di eventuali problemi giuridici relativi alla posizione contrattuale in essere (ad esempio Avvocatura distrettuale e generale dello Stato, ai fini della gestione del contenzioso penale, civile ed amministrativo)
-soggetti terzi per finalità legate all'attività istituzionale(es.collaboratori organizzazioni esterne,ecc.)
- a tutti i soggetti eventuali destinatari delle campagne di comunicazione del Conservatorio
I dati potranno essere comunicati anche a soggetti pubblici non economici quando la comunicazione è necessaria per lo svolgimento delle funzioni istituzionali dell'ente richiedente.

7) Esistenza di un processo decisionale automatizzato, compresa la profilazione
L'IRSAP non adotta alcun processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del Regolamento UE n. 679/2016.

8) Diritti dell'interessato
In ogni momento, l'interessato può esercitare, ai sensi dell'art. 7 del D.Lgs. 196/2003 e degli articoli dal 15 al 22 del Regolamento UE n. 2016/679, il diritto di:
a) chiedere la conferma dell'esistenza o meno di propri dati personali;
b) ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;
c) ottenere la rettifica e la cancellazione dei dati;
d) ottenere la limitazione del trattamento;
e) ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti;
f) opporsi al trattamento in qualsiasi momento ed anche nel caso di trattamento per finalità di marketing diretto;
g) opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.
h) chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
i) revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) proporre reclamo a un'autorità di controllo.
Per l'esercizio dei predetti diritti è possibile inoltrare richiesta scritta inviata al Titolare del trattamento (IRSAP) all'indirizzo postale via E. Ferruzza Sud/Ovest 1/5, 90124 Palermo o all'indirizzo mail: info@irsapsicilia.it

9) Acquisizione del consenso e conseguenze del mancato conferimento
Il conferimento dei dati deve ritenersi obbligatorio per quanto riguarda i trattamenti che l'Istituto deve effettuare per adempiere alle proprie obbligazioni istituzionali nei confronti dell'interessato sulla base del rapporto in essere, nonché in base ad obblighi di leggi, norme, regolamenti riportati a mero titolo esemplificativo nei punti 5.a), 5.b), 5.c), 5.d).
Il mancato consenso o la revoca del consenso al trattamento di tali dati comporta l'impossibilità per l'IRSAP di dar corso al rapporto in essere o di fornire il servizio richiesto.

= = = = = = = = = =

ACQUISIZIONE DEL CONSENSO

Io sottoscritto/a _____ in qualità di_____ _____dichiaro di aver ricevuto, letto e compreso l'informativa che precede.
A tal fine io sottoscritto/a _____ _____esprimo in modo consapevole, libero ed autonomo il consenso al trattamento dei dati personali per le finalità esplicitate a titolo esemplificativo ai punti 5.a), 5.b), 5.c), 5.d)
[ ] esprimo il consenso [ ] nego il consenso

Luogo e data _____, ___ / ___/ _____

Firma
_____