Procedura Adempimenti Privacy

Cisterna di Latina 01 marzo 2022

Sommario

1. Premessa

Il Regolamento Europeo 679/16 - di seguito GDPR – e il Codice in materia di protezione dei dati personali - Decreto legislativo 30 giugno 2003, n. 196, novellato dal Decreto legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 mirano alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Gelit ha implementato la seguente ed altre procedure per garantire la tutela di tutte le persone fisiche con le quali la società stessa e i suoi referenti si interfacciano nello svolgimento delle attività lavorative.
In particolare, la procedura disciplina i seguenti aspetti legati agli adempimenti privacy che devono essere svolti in occasione di:

- Inizio e fine di un rapporto di lavoro;
- Inizio e fine di un rapporto commerciale con clienti / fornitori / consulenti;
- Ingresso di visitatori / trasportatori;
- Inizio e fine del rapporto con Amministratori, Sindaci e membri dell'Organismo di Vigilanza;
- Sponsorizzazioni, donazioni e liberalità generiche;
- Gestione moduli consensi per riprese video fotografiche;
- Gestione del Registro dei trattamenti;
- Gestione uffici e archivi cartacei ed elettronici;
- Gestione dei curricula vitae;
- Aggiornamento della normativa Privacy di riferimento;
- Aggiornamento della documentazione Privacy.

Nei paragrafi successivi vengono esposte le modalità di gestione delle attività di cui sopra, i referenti aziendali coinvolti e le relative responsabilità.

Si ricorda che tutti gli aspetti IT sono regolamentati dal *Regolamento IT* al quale si rimanda per la gestione di tutti gli aspetti legati alle misure tecniche-informatiche che la società ha in essere.

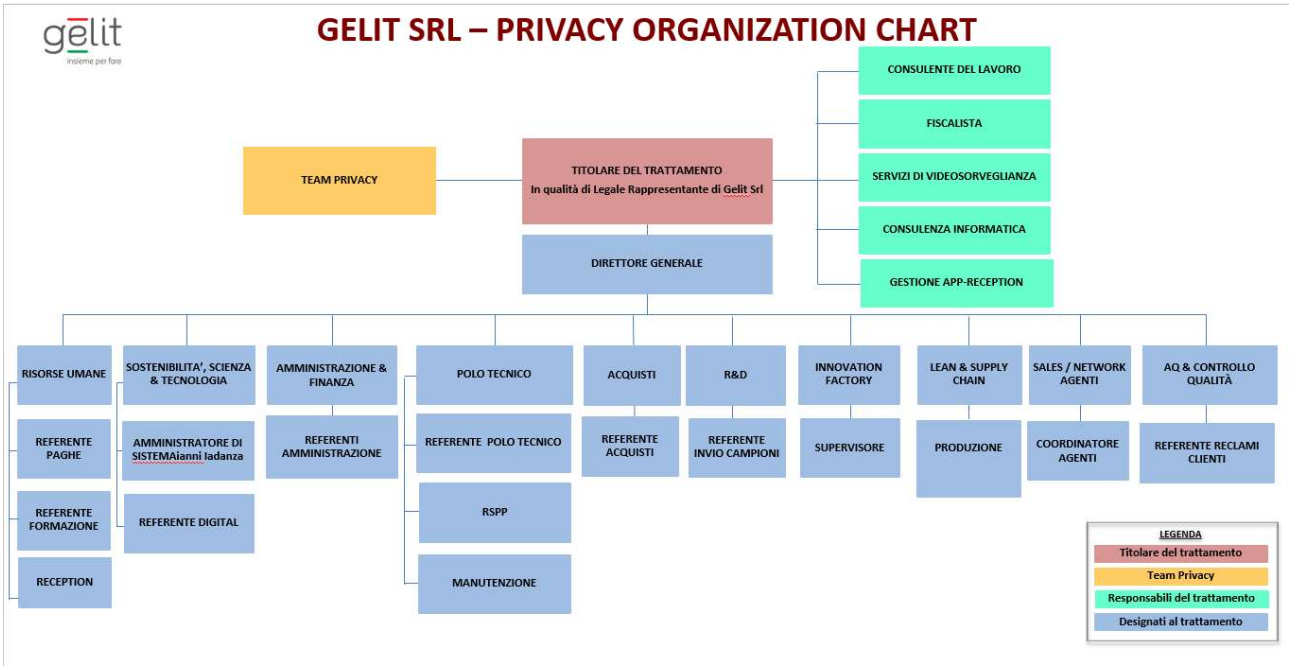
2. Organizzazione Privacy

La struttura organizzativa Privacy è stata definita dal Titolare, nella figura del Rappresentante Legale, in fase di implementazione della normativa di riferimento.

L'organigramma privacy risulta così strutturato:

- Al vertice vi è la figura del Titolare, coadiuvato dal Team Privacy;
- Al Titolare riportano i Designati al Trattamento;
- Al Titolare riportano i Responsabili del Trattamento.

L'organigramma Privacy di seguito riportato viene affisso in bacheca dal Team Privacy che in caso di modifiche deve provvedere a mantenere evidenza delle eventuali modifiche apportate.



Ogni soggetto di cui sopra ha ricevuto una nomina da parte del Titolare che riporta i dati e i trattamenti che lo stesso può gestire, i compiti e le responsabilità assegnate, le istruzioni cui attenersi nella gestione dei dati e del trattamento.
Le nomine sono formalizzate in appositi documenti e sono firmate dal Titolare e dal soggetto destinatario della nomina per accettazione.
Il Team Privacy deve anche garantire che tutte le nomine ritornino debitamente firmate dal diretto interessato e provvedere in caso di nuovi dati e trattamenti ad aggiornare le nomine relative ed in caso di modifiche alla struttura organizzativa (es. inserimento di nuove funzioni, cessazione di un designato, sostituzione ,..) provvedere al relativo aggiornamento delle nomine stesse.
Copia del documento è conservato nelle cartelle personali di ogni dipendente a cura del Responsabile Risorse Umane e in apposita directory in rete, a cura del Team Privacy, accessibile, tramite credenziali, solo dal Titolare e dal Team Privacy.

Per le attività legate ai Responsabili del Trattamento si rimanda al paragrafo “Gestione Responsabili del Trattamento”.

3. Instaurazione nuovo rapporto di lavoro

In fase di instaurazione di un nuovo rapporto di lavoro è compito del Responsabile Risorse Umane, coadiuvato dal Team Privacy:

- Consegnare al dipendente il documento “Gelit informazione e acquisizione del consenso per il trattamento dei dati personali dei dipendenti” con le indicazioni relative ai dati trattati e ai trattamenti gestiti, nonché con le informazioni in merito ai diritti esercitabili dall’interessato, l’indicazione di chi può trattare i suoi dati e i soggetti nominati Responsabili del Trattamento. In particolare, è necessario informare il dipendente che per il trattamento di alcuni suoi dati personali, prevalentemente immagini a lui riconducibili, occorre che lo stesso presti il consenso al trattamento in quanto senza il suo consenso il Titolare non potrà effettuare o sarà limitato nei trattamenti specifici

per cui si richiede il consenso; occorre anche informare il dipendente delle possibili implicazioni derivanti dal rifiuto del suo consenso.

Inoltre, occorre specificatamente informare l'interessato che i suoi dati saranno gestiti, oltre che dal Titolare del Trattamento e dai designati, anche da alcuni Responsabili ed in particolare:

- la società al quale la società ha esternalizzato l'elaborazione dei cedolini;
- il Medico Competente al quale la società ha affidato gli adempimenti in materia di sorveglianza sanitaria ai sensi del D.Lgs 81/08;
- la società alla quale la società ha affidato la gestione del servizio di reception e videosorveglianza al di fuori del normale orario di lavoro;
- eventuali altri soggetti cui la società trasferisce /deciderà di trasferirei dati dell'interessato e a cui ha affidato /affiderà la gestione.

Il documento "Gelit informazione e acquisizione del consenso per il trattamento dei dati personali dei dipendenti" deve essere consegnato in duplice copia al dipendente; una copia deve ritornare firmata per presa visione e deve essere archiviata nella cartella personale del singolo dipendente.

- Valutare, unitamente al Titolare del Trattamento, nella persona del Rappresentante Legale, la necessità di nominare il dipendente quale Designato al Trattamento (o l'eventuale suo inserimento all'interno del Team Privacy). Tale valutazione deve essere fatta tenendo in considerazione il ruolo del dipendente / collaboratore, le tipologie di dati che dovranno essere gestiti nello svolgimento delle sue mansioni, nonché i trattamenti che saranno effettuati. Nel caso in cui sia necessario predisporre una nomina, la stessa dovrà essere predisposta dal Team Privacy, verificata e firmata dal Titolare del Trattamento e consegnata al nuovo Designato / membro del Team Privacy con la richiesta di controfirmarla per accettazione. Tutte le nomine a Designati devono essere archiviate coerentemente con quanto definito nel capitolo "2. Organizzazione Privacy". Inoltre, nel caso in cui il dipendente / collaboratore venga nominato Designato, lo stesso dovrà essere formato sugli aspetti delle procedure privacy che lo riguardano direttamente anche attraverso la consegna della brochure formativa "Formazione Gelit (designati)". Invece, se un dipendente dovesse entrare a far parte del Team Privacy allo stesso dovranno essere rese disponibili le procedure relative alla gestione del Data Breach, alla gestione dei diritti degli interessati, alla gestione degli adempimenti Privacy e alla gestione della valutazione dell'impatto Privacy e dovrà essere consegnata la brochure formativa "Formazione Gelit (Team Privacy)" che costituisce l'oggetto della formazione in materia di Privacy come sotto specificato.
- Consegnare a tutti i dipendenti il documento "Regolamento IT" contenente le indicazioni in merito all'utilizzo dei sistemi e degli strumenti informatici resi disponibili per lo svolgimento dell'attività lavorativa. Tale documento è inserito nella lista della documentazione resa disponibile ad ogni nuovo dipendente / collaboratore e deve essere firmata dallo stesso per ricezione, presa visione ed accettazione. Inoltre, dovrà essere consegnata la brochure formativa "Formazione Gelit (dipendenti)".

La documentazione cartacea ed elettronica relativa al dipendente / collaboratore deve essere gestita nel rispetto di quanto previsto dal paragrafo "Gestione Uffici ed Archivi".

In fase di instaurazione di un nuovo rapporto di lavoro, il Responsabile Risorse Umane in collaborazione con il Team Privacy è tenuto ad organizzare un momento di formazione per quei neo assunti che dovranno gestire dati personali o particolari di soggetti terzi. Tale formazione è mirata a informare il nuovo assunto sugli aspetti chiave della normativa sulla protezione dei dati personal, presentare la tipologia di dati e trattamenti

che lo stesso potrebbe trovarsi a gestire, presentare le misure tecniche ed organizzative implementate dalla società al fine di garantire la compliance al GDPR e al Codice in materia di protezione dei dati personali, esplicitare le principali linee di condotta che Gelit segue nella gestione dei dati personali.

Durante tutto il processo di instaurazione di un nuovo rapporto di lavoro il Team Privacy deve garantire che gli adempimenti previsti vengano effettivamente svolti in modo che il nuovo assunto comprenda chiaramente gli aspetti legati alla privacy.

4. Cessazione rapporto di lavoro

In caso di cessazione del rapporto di lavoro con un dipendente / collaboratore, è compito del Responsabile Risorse Umane conservare tutta la documentazione relativa al dipendente / collaboratore per un periodo di dieci anni dopo il termine del rapporto di lavoro ad eccezione dei casi in cui siano in corso contestazioni con il dipendente per cui tutta la documentazione relativa al rapporto di lavoro verrà conservata fino ai 10 anni successivi la risoluzione del contenzioso.
Trascorso tale tempo, il Responsabile Risorse Umane dovrà provvedere alla cancellazione o a dare disposizioni per la cancellazione (sia dai dispositivi informatici sia a livello cartaceo) di qualsiasi dato relativo al dipendente.
Qualora il Titolare riceva una richiesta di esercizio dei diritti da parte di un interessato dipendente cessato, le attività inerenti al soddisfacimento della richiesta dovranno essere prese in carico e svolte dal Responsabile Risorse Umane con l'eventuale supporto del Responsabile IT, laddove la richiesta dovesse richiedere anche un intervento sui sistemi informativi.
È compito del Team Privacy verificare il rispetto di tali adempimenti nonché il corretto soddisfacimento del diritto.
La documentazione cartacea ed elettronica inerente questo evento deve essere gestita nel rispetto di quanto previsto dal paragrafo "Gestione Uffici ed Archivi".

5. Inizio di un nuovo rapporto commerciale con clienti / fornitori / consulenti

In occasione dell'inizio di un nuovo rapporto commerciale con clienti, fornitori o consulenti, è importante che la persona Gelit che ha il primo contatto con l'interessato, lo informi sulle modalità di trattamento dei dati personali da parte di Gelit, sui diritti dell'interessato e delle modalità di esercizio degli stessi. Per far questo il referente aziendale che si interfaccia con clienti, fornitori, consulenti provvedere ad inserire frase negli ordini / contratti / corrispondenza scambiata con i soggetti esterni e il link che rimanda all'informativa sul trattamento dei dati e ad informando della mail da contattare su tematiche inerenti la protezione dei dati personali (eventuale esercizio dei diritti o segnalazioni di violazioni).

I dati personali relativi al cliente / fornitore / consulente sono gestite:

- Dal Responsabile e dai referenti dell'Ufficio Amministrativo per tutti gli aspetti relativi alla gestione delle anagrafiche: in particolare, sono gestiti dati di contatto, dati identificativi, dati economici – patrimoniali e finanziari;
- Dalla Direzione Generale e da tutti gli altri Uffici che a vario titolo si interfacciano con il soggetto terzo. I dati gestiti sono solo di contatto.

Nei documenti “Gelit Informazione per il trattamento dei dati personali dei clienti” o “Gelit Informazione per il trattamento dei dati personali dei fornitori e consulenti” sopra menzionati sono indicati i diritti esercitabili dagli Interessati.
Gli adempimenti correlati alla gestione dei diritti degli interessati sono riportati nella procedura *Esercizio Diritti Interessato*.
Tutta la documentazione cartacea ed elettronica relativa a clienti, fornitori e consulenti deve essere gestita nel rispetto di quanto previsto dal paragrafo “Gestione Uffici e Archivi”.

6. Termine del rapporto commerciale con clienti / fornitori / consulenti

In caso di termine del rapporto commerciale con clienti / fornitori / consulenti, è responsabilità dell’Ufficio Amministrativo e dei vari Responsabili di funzione, ognuno secondo le specifiche finalità previste nell’ambito del proprio ruolo conservare la documentazione relativa ai clienti / fornitori / consulenti per un periodo di dieci anni dopo il termine del rapporto commerciale ad eccezione dei casi in cui siano in corso contestazioni con le terze parti per cui tutta la documentazione relativa al rapporto commerciale verrà conservata fino ai 10 anni successivi la risoluzione del contenzioso.
Trascorso tale tempo, il Responsabile Amministrativo e i vari Responsabili di funzione dovranno provvedere alla cancellazione o a dare disposizioni per la cancellazione (sia dai dispositivi informatici sia a livello cartaceo) di qualsiasi dato relativo alle terze parti interessate.
Laddove la richiesta dovesse richiedere anche un intervento sui sistemi informativi, dovrà essere coinvolto il Responsabile IT.
Tutta la documentazione cartacea ed elettronica relativa a clienti, fornitori e consulenti deve essere gestita nel rispetto di quanto previsto dal paragrafo “Gestione Uffici e Archivi”.
È compito del Team Privacy verificare il rispetto di tali adempimenti.

7. Ingresso di visitatori / trasportatori

In fase di ingresso di visitatori e trasportatori il documento “Gelit Informazione trasportatori e visitatori” è reso disponibile tramite l’AppReception attraverso la quale i visitatori e i trasportatori sono tenuti a registrare il loro ingresso. In particolare, le informazioni richieste al visitatore / trasportatore sono relative a dati anagrafici (nome e cognome), dati identificativi (carta identità o patente di guida), dati su rapporti professionali in essere (es. società di appartenenza) e altri dati (orario di ingresso ed uscita). Inoltre, eventuali immagini sono riprese del sistema di videosorveglianza.
Tali informazioni sono gestite dal referente della reception sotto la responsabilità del Responsabile Risorse Umane cui la funzione risponde, in apposito documento elettronico gestito tramite l’applicazione AppReception il cui fornitore è stato nominato Responsabile del Trattamento.
I dati relativi a visitatori e trasportatori sono conservati su supporto elettronico per il periodo stabilito nel documento “Gelit Informazione trasportatori e visitatori” ed in particolare i dati relativi agli accessi vengono cancellati dopo 3 anni dall’avvenuto accesso, mentre le riprese del sistema di videosorveglianza non vengono registrate se l’accesso avviene durante le ore diurne in quanto la registrazione su supporto digitale avviene solo dalle ore 22.00 alle ore 6.00.
Tutta la documentazione elettronica relativa a trasportatori e visitatori deve essere gestita nel rispetto di quanto previsto dal paragrafo “Gestione Uffici e Archivi”.
E’ compito del Team Privacy verificare il rispetto di tali adempimenti.

8. Rapporto con Amministratori, Sindaci e membri dell'Organismo di Vigilanza

A tutti i membri degli organi sociali e di controllo deve essere consegnato il documento "Gelit Informazione Amministratori, Sindaci e membri dell'OdV" da parte del Responsabile Amministrativo.
I dati personali di Amministratori, Sindaci e membri dell'OdV sono gestiti dal Responsabile e dai referenti dell'Ufficio Amministrativo per tutti gli aspetti relativi alla gestione degli adempimenti societari, alla registrazione delle fatture e relativi pagamenti, nonché per tutti gli adempimenti fiscali: in particolare, sono gestiti dati di contatto, dati identificativi, dati economici – patrimoniali e finanziari.
Nel documento "Gelit Informazione Amministratori, Sindaci e membri dell'OdV" sopra menzionati sono indicati i diritti esercitabili dagli Interessati.
Gli adempimenti correlati alla gestione dei diritti degli interessati sono riportati nella procedura *Esercizio Diritti Interessato*.
Tutta la documentazione cartacea ed elettronica relativa a clienti, fornitori e consulenti deve essere gestita nel rispetto di quanto previsto dal paragrafo "Gestione Uffici e Archivi".
Al termine del rapporto con Amministratori, Sindaci e membri dell'OdV, è responsabilità dell'Ufficio Amministrativo conservare la documentazione relativa ad Amministratori, Sindaci e membri dell'OdV per un periodo di dieci anni dopo il termine dell'incarico di membro dell'organo societario ad eccezione dei casi in cui siano in corso contestazioni con le terze parti per cui tutta la documentazione relativa al rapporto dell'incarico di membro dell'organo societario verrà conservata fino ai 10 anni successivi la risoluzione del contenzioso.
Trascorso tale tempo, il Responsabile Amministrativo dovrà provvedere alla cancellazione o a dare disposizioni per la cancellazione (sia dai dispositivi informatici sia a livello cartaceo) di qualsiasi dato relativo alle terze parti interessate.
Laddove la richiesta dovesse richiedere anche un intervento sui sistemi informativi, dovrà essere coinvolto il Responsabile IT.
Tutta la documentazione cartacea ed elettronica relativa a Amministratori, Sindaci e membri dell'OdV deve essere gestita nel rispetto di quanto previsto dal paragrafo "Gestione Uffici e Archivi".
È compito del Team Privacy verificare il rispetto di tali adempimenti.

9. Sponsorizzazioni, Donazioni e Liberalità Generiche

In occasione del riconoscimento di sponsorizzazioni, donazioni e liberalità generiche ad associazioni, ONLUS o società sportive è importante che la persona Gelit che ha il primo contatto con l'interessato, lo informi sulle modalità di trattamento dei dati personali da parte di Gelit, sui diritti dell'interessato e delle modalità di esercizio degli stessi. Per far questo il referente aziendale che si interfaccia con tali enti deve consegnare il documento "Gelit Informazione per il trattamento dei dati personali di Associazioni, ONLUS, Società Sportive".

I dati personali relativi alle Associazioni, ONLUS, Società Sportive sono gestite:

- dal Responsabile e dai referenti dell'Ufficio Amministrativo per tutti gli aspetti relativi alla gestione amministrativa della sponsorizzazione, donazione o liberalità: in particolare, sono gestiti dati di contatto, dati identificativi, dati economici – patrimoniali e finanziari;

- dalla Direzione Generale e da tutti gli altri Uffici che a vario titolo si interfacciano con il soggetto terzo. I dati gestiti sono solo di contatto.

Nel documento "Gelit Informazione per il trattamento dei dati personali di Associazioni, ONLUS, Società Sportive" sopra menzionato sono indicati i diritti esercitabili dagli Interessati.
Gli adempimenti correlati alla gestione dei diritti degli interessati sono riportati nella procedura *Esercizio Diritti Interessato*.
Tutta la documentazione cartacea ed elettronica relativa a Associazioni, ONLUS, Società Sportive deve essere gestita nel rispetto di quanto previsto dal paragrafo "Gestione Uffici e Archivi".
La documentazione viene conservata 10 anni.

10. Gestione moduli consensi per riprese video fotografiche

Il Team Privacy ha il compito, nel caso di feste o eventi aziendali, di raccogliere i consensi da parte degli invitati agli eventi. Tale consenso va raccolto attraverso uno specifico modulo denominato "Informazione e consenso agli eventi". Il seguente modulo va consegnato agli invitati in prossimità dell'evento e deve essere firmato e riconsegnato alla società almeno 2/3 giorni prima dell'evento. Queste tempistiche vanno rispettate in modo da consentire al team che si occupa dell'organizzazione dell'evento di capire e organizzare al meglio l'evento stesso e le riprese video fotografiche garantendo il rispetto delle specifiche scelte in termini di acquisizione di immagini riconducibili all'interessato da parte di ogni partecipante l'evento.
Qualora vi sia la possibilità che all'evento partecipino minori di 14 anni, va consegnato il modulo "Informazione e consenso minori invitati agli eventi", al soggetto che detiene la patria potestà. Tale modulo, deve essere compilato in tutte le sue parti, firmato e consegnato 2/3 giorni prima dell'evento per le ragioni organizzative citate sopra.
Il consenso da parte dell'interessato deve essere esplicitato per ogni singolo evento. Per questo il team privacy si assicurerà che tali moduli vengano diffusi e raccolti con esplicitazione del consenso per ogni singolo partecipante e per ogni evento aziendale in programma.
E' responsabilità del Team Privacy provvedere alla conservazione dei consensi per un periodo di dieci anni dopo il termine dell'evento ad eccezione dei casi in cui siano in corso contestazioni con le terze parti per cui tutta la documentazione relativa al rapporto commerciale verrà conservata fino ai 10 anni successivi la risoluzione del contenzioso.
Trascorso tale tempo, il Team Privacy dovrà provvedere alla cancellazione (sia dai dispositivi informatici sia a livello cartaceo) di qualsiasi dato relativo alle terze parti interessate.
Laddove la richiesta dovesse richiedere anche un intervento sui sistemi informativi, dovrà essere coinvolto il Responsabile IT.

11. Gestione Uffici e archivi

Tutti gli uffici si trovano in edifici protetti da un sistema anti-intrusione. Ogni dipendente è dotato di un codice personale per attivare/disattivare l'allarme in modo tale da garantire che gli accessi fisici ai vari edifici, e di conseguenza ai vari uffici, siano consentiti solo al personale dipendente che appartiene allo specifico ufficio.

Il sistema di accesso con utilizzo del codice di allarme consente di gestire un log degli accessi, mantenendo traccia dei codici di ingresso e dell'ora di ingresso nei vari edifici.
Ogni designato deve garantire che i dati personali e particolari gestiti dallo stesso ed eventualmente dai dipendenti del proprio ufficio siano adeguatamente protetti nel rispetto di quanto previsto dalla normativa.
In particolare:

- Il Responsabile Risorse Umane e gli addetti all'ufficio sono tenuti a chiudere sempre a chiave il proprio ufficio, quando si allontanano dall'ufficio stesso. Inoltre, tutti gli armadi dove sono conservati i documenti relativi a dipendenti devono essere chiusi a chiave. A fine giornata lavorativa sulla scrivania di ogni addetto all'ufficio sopra menzionato non devono essere lasciati documenti con dati personali e/o particolari: tutti i documenti devono essere riposti negli appositi raccoglitori e negli armadi. I referenti dell'Ufficio Risorse Umane hanno una chiave a loro disposizione.
- Il Responsabile Amministrativo e i referenti amministrativi sono tenuti a chiudere gli armadi o l'ufficio quando nessuno è presente presso l'ufficio stesso. A fine giornata lavorativa sulla scrivania non devono essere lasciati documenti con dati personali e/o particolari: tutti i documenti devono essere riposti negli appositi raccoglitori e negli armadi.
- Ai responsabili e referenti di tutti gli altri uffici è richiesto di archiviare i documenti che contengono dati personali e/o particolari in appositi raccoglitori e di conservarli negli armadi chiusi a chiave. A fine giornata lavorativa sulla scrivania non devono essere lasciati documenti con dati personali e/o particolari: tutti i documenti devono essere riposti negli appositi raccoglitori e negli armadi.

Tutti i contratti con clienti e fornitori che contengono dati personali e particolari devono essere archiviati presso l'ufficio Amministrativo che ne assicura la riservatezza.
Eventuali fotocopie devono essere trattate e conservate con le stesse modalità dei documenti originali.

La distruzione di documenti cartacei contenenti dati particolari deve avvenire tramite i "trita documenti" disponibili presso l'ufficio Risorse Umane e l'ufficio Amministrazione.

Per quanto riguarda la gestione della documentazione elettronica la stessa è archiviata in directory elettroniche organizzate secondo i seguenti criteri di sicurezza logica:

- Le directory con i dati dei dipendenti sono accessibili al solo Responsabile Risorse Umane e agli addetti all'ufficio Risorse Umane;
- Ogni ufficio è dotato di directory riservate alle quali possono accedere solo i referenti dell'Ufficio stesso a seconda delle specifiche necessita derivanti dal ruolo svolto da ognuno.

Nel caso in cui la documentazione contenente dati personali e particolari sia archiviata nelle cartelle di outlook, deve essere garantito idoneo livello di protezione.
Le modalità di protezione dei dati dal punto di vista informatico sono riportate nel documento "Regolamento IT" al quale si rimanda per tutti i dettagli.
Ai fini di questa procedura, si sottolinea che:

- E' consentito l'accesso su ogni computer solo tramite l'inserimento di user id e password dedicata a ciascun utente;
- La USERID è personale e non cedibile ad altri utenti;
- Ogni volta che si lascia la propria postazione lavorativa è necessario attivare il blocco del pc.

La sala server è accessibile solo all'amministratore di sistema attraverso utilizzo di apposita chiave della sala server che è detenuta solo dal Responsabile IT.

Gestione archivi con i dati di interessati – dipendenti/collaboratori – cessati

Per quanto riguarda la gestione dei dati personali e particolari di dipendenti / collaboratori cessati il Responsabile Risorse Umane:

- Per i dati riportati su documenti cartacei deve assicurare che gli archivi cartacei siano chiusi a chiave in locale accessibile solo al Responsabile Risorse Umane o in locale accessibile a personale limitato / identificato a priori;
- Per i dati riportati su documenti elettronici deve assicurare che gli archivi elettronici siano protetti dalle misure di sicurezza logica che garantiscano l'accesso al solo Responsabile Risorse Umane.

In ogni caso, tutti i dati relativi a dipendenti cessati devono essere cancellati nel rispetto di quanto riportato al paragrafo "Cessazione rapporto di lavoro".

Gestione archivi con i dati di interessati – fornitori, consulenti, clienti, visitatori, trasportatori - cessati

Per quanto riguarda la gestione dei dati personali e particolari di clienti/fornitori/consulenti cessati il Responsabile Amministrativo:

- Per i dati riportati su documenti cartacei deve assicurare che gli archivi cartacei siano chiusi a chiave in locale accessibile solo ai referenti dell'Ufficio Amministrativo o in locale accessibile a personale limitato / identificato a priori;
- Per i dati riportati su documenti elettronici deve assicurare che gli archivi elettronici siano protetti dalle misure di sicurezza logica che garantiscano l'accesso ai referenti dell'Ufficio Amministrativo.

In ogni caso, tutti i dati relativi a clienti/fornitori/consulenti con i quali non si hanno più relazioni commerciali devono essere cancellati nel rispetto di quanto riportato al paragrafo "Cessazione rapporto commerciale", "Ingresso di visitatori / trasportatori" e "Gestione moduli consensi per riprese video fotografiche".

12. Gestione dei curricula vitae

I CV possono essere ricevuti:

- Direttamente dal Responsabile Risorse Umane in formato cartaceo o elettronico;
- Dai referenti di altri uffici, in formato cartaceo o elettronico, che sono tenuti a consegnarlo al Responsabile Risorse Umane. In caso di documento elettronico, è richiesto di provvedere alla cancellazione del documento stesso dalla mail (sia di ricezione che di invio) o dall'eventuale supporto elettronico nel quale è salvato il cv elettronico;
- Dai referenti della reception, in formato cartaceo, che sono tenuti a consegnare il documento al Responsabile Risorse Umane.

Si ricorda che tutti i cv cartacei devono essere consegnati dal candidato in busta chiusa. Nel caso in cui il candidato si presenti senza busta, i referenti della reception o qualsiasi referente di altro ufficio dovrà inserire il cv in una busta riservata al Responsabile Risorse Umane.
Il Responsabile Risorse Umane provvederà a conservare i CV nel rispetto di quanto previsto dal paragrafo "Gestione Uffici ed Archivi".

Nel rispetto di quanto previsto dall'articolo 111-bis (Informazioni in caso di ricezione di curriculum) del Decreto legislativo 30 giugno 2003, n. 196, novellato dal Decreto legislativo 10 agosto 2018, n. 101, "*le informazioni di cui all'articolo 13 del Regolamento in merito alle informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto*

utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto".
È responsabilità del Responsabile Risorse Umane informare i candidati circa le modalità di trattamento dei dati raccolti tramite CV, attraverso la consegna del documento "Gelit Informazione e Consenso candidati".

Cancellazione cv:
Il Responsabile Risorse Umane è tenuto a cancellare i CV ricevuti in formato elettronico e a distruggere i CV cartacei, per i quali non si è concretizzata un'assunzione, dopo XX anni dal loro ricevimento.
I CV dei canditati assunti vengono invece conservati tra la documentazione personale del dipendente e come tale archiviate e conservata nella cartella personale di ciascun dipendente e pertanto per la cancellazione dei dati personali si seguono le regole previste dal paragrafo "Cessazione del Rapporto di Lavoro".
È richiesto a tutti i responsabili di funzione che a vario titolo sono coinvolti nel processo di selezione di candidati di conservare i dati personali del candidato nel rispetto di quanto previsto dal paragrafo "Gestione Uffici ed Archivi"; in particolare, i CV ricevuti, sia in formato elettronico che cartaceo, relativi a candidati non selezionati devono essere cancellati/ distrutti dopo 3 anni dal loro ricevimento. I CV relativi a candidati assunti vengono conservati nel fascicolo dipendenti e verranno distrutti, con tutta l'altra documentazione riguardante il rapporto di lavoro, dieci anni dopo il termine del rapporto di lavoro ad eccezione dei casi in cui sono in corso contestazioni con il dipendente per cui tutta la documentazione relativa al rapporto di lavoro verrà conservata fino alla risoluzione del contenzioso.

13. Gestione dei Responsabili del Trattamento

I Responsabili del trattamento sono soggetti cui il Titolare ha esternalizzato la gestione di uno o più trattamenti.
La nomina a Responsabile del Trattamento viene firmata dal Titolare del Trattamento e deve contenere i seguenti elementi:

- Elenco trattamenti;
- Tipo di dati personali trattati;
- Obblighi del titolare;
- Obblighi del responsabile del trattamento.

Copia della nomina, firmata per accettazione da parte del Responsabile del Trattamento, viene archiviata a cura del Team Privacy in apposito faldone cartaceo e in apposita directory di rete accessibile, tramite credenziali, solo dal Titolare e dal Team Privacy.

Modifica
Nel caso in cui ci sia la necessità di provvedere alla modifica della nomina a Responsabile del Trattamento, è compito del Titolare coadiuvato dal Team Privacy identificare le modifiche da apportare. La nomina dovrà essere firmata dal Titolare e per accettazione dal Responsabile del Trattamento.

Verifica degli adempimenti relativi ai Responsabili del Trattamento
È compito del Titolare, supportato dal Team Privacy, interfacciarsi con il Responsabile del Trattamento per verificare il rispetto degli obblighi di quest'ultimo riportati nella nomina.

14. Gestione del Registro dei Trattamenti

Il registro dei trattamenti è previsto dal Regolamento Europeo all'articolo 30 ed è definito come "registro delle attività di trattamento svolte sotto la responsabilità del Titolare del Trattamento".
Il Registro del Trattamento deve contenere almeno le seguenti informazioni:

- Il nome e i dati di contatto del titolare del trattamento;
- Il trattamento e le finalità del trattamento;
- Ove applicabile, il contitolare del trattamento;
- La tipologia di dati personali e/o particolati trattati;
- Una descrizione delle categorie di interessati e la legittimazione al trattamento;
- Ove applicabile, il responsabile del trattamento e/ designato;
- Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- La descrizione delle modalità e criteri di archiviazione dei dati personali;
  Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative in essere.

Il registro del trattamento viene conservato in formato elettronico da parte del Titolare; è mantenuta anche una copia cartacea che viene firmata e datata dal Titolare.

E' compito del Titolare, supportato dal Team Privacy, garantire l'aggiornamento del registro dei trattamenti con frequenza almeno annuale al fine di verificare che le informazioni riportate nel Registro dei Trattamenti siano coerenti e corrette sulla base dei trattamenti gestiti e delle responsabilità assegnate in termini di protezione dei dati personali.
Inoltre, in caso di nuovi dati e trattamenti gestiti dalla società, il Titolare, supportato dal Team Privacy, deve garantire il corretto inserimento dei nuovi dati e trattamenti nel Registro dei Trattamenti aggiornando per lo specifico trattamento tutte le informazioni sopra specificate.

Al termine dell'attività di aggiornamento il registro dovrà essere stampato, firmato e datato dal Titolare del Trattamento.

In caso di modifiche alla normativa di riferimento che hanno impatto sul Registro dei Trattamenti, è responsabilità del Titolare, supportato dal Team Privacy, apportare le modifiche necessarie.
A modifiche ultimate, il Titolare dovrà provvedere a stampare, firmare e datare il documento stesso e a conservarne copia elettronica.

15. Gestione richieste di esercizio dei diritti da parte degli interessati

È compito del Team Privacy visionare con cadenza periodica la mail dedicata privacy@gelit.it al fine di verificare il ricevimento di eventuali segnalazioni da parte degli interessati per l'esercizio dei propri diritti.
Il Team Privacy dovrà inoltre compilare l'apposito registro delle richieste pervenute. Per ulteriori dettagli si rimanda a quanto citato nella procedura "Esercizio Diritti Interessato".

16. Gestione dei Data Breach

È compito del Team Privacy gestire il processo in caso di eventuali violazioni dei dati personali secondo quanto previsto dalla procedura "Procedura Data Breach", cui si rimanda per tutti i dettagli.

17. Gestione Personal data risk assessment e PIA

È compito del Team Privacy con cadenza periodica la valutazione del rischio privacy e la PIA al fine di garantire la costante adeguatezza del sistema privacy a quanto previsto dalla normativa. Per ulteriori dettagli si rimanda a quanto citato nella procedura "Procedura PIA".

18. Aggiornamento della normativa

In caso di aggiornamento / modifiche alla normativa di riferimento, è compito del Titolare al trattamento, coadiuvato dal Team Privacy:

- Provvedere alla verifica che le attività e i documenti esplicitati nella presente procedura mantengano la conformità alle modifiche intervenute alla normativa. In particolare, dovrà essere verificato il contenuto dei documenti di Informazione, nomine e il Registro dei Trattamenti;
- Provvedere a diffondere a tutti gli interessati i documenti modificati;
- Provvedere alla formazione del personale in merito alle modifiche introdotte dalla normativa e di conseguenza ai documenti aggiornati.

19. Aggiornamento della documentazione

È compito del Titolare al trattamento, coadiuvato dal Team Privacy provvedere all'aggiornamento di tutta la documentazione privacy (informative, nomine, registri dei trattamenti, procedure), al fine di rispettare i principi definiti dal regolamento di "privacy by design" e "privacy by default", in caso di:

- Modifiche normative;
- Nuovi dati trattati o nuovi trattamenti;
- Modifiche alla struttura Privacy.

Tutti i documenti modificati dovranno resi disponibili ai designati con particolare attenzione ai documenti "Gelit Informazione e Consenso dipendenti ", "Gelit Informazione fornitori consulenti", "Gelit Informazione trasportatori e visitatori", "Gelit Informazione clienti" che dovranno essere distribuire ai Designati, con richiesta specifica da parte del Team Privacy di provvedere alla cancellazione delle precedenti informative, affinché gli stessi possano utilizzare i documenti aggiornati nello svolgimento delle specifiche attività quotidiane.

Il titolare del trattamento al fine di dare evidenza delle attività di aggiornamento eseguite, dei documenti utilizzati, nonché dei piani di adeguamento in essere e chiusi, provvede, con il supporto del team Privacy, alla archiviazione e conservazione della documentazione medesima.

20. Privacy: area del fare e del non fare

Al Team Privacy è richiesto di:

- Supportare il Titolare nello svolgimento delle sue attività legate alle tematiche Privacy;

- Seguire le istruzioni impartite dal Titolare in merito alle misure di sicurezza fisiche e logiche per garantire la sicurezza dei dati;
- Impartire ai designati le istruzioni in merito alle misure di sicurezza fisiche e logiche per garantire la sicurezza dei dati da loro gestiti sulla base di quanto definito dal Titolare;
- Attivarsi nei modi e nei tempi previsti dalle procedure privacy specifiche atte a garantire la corretta gestione dei dati personali in linea con la normativa di riferimento.

A tutti i designati al Trattamento è richiesto di seguire le istruzioni impartite dal Titolare in merito alle misure di sicurezza fisiche e logiche per garantire la sicurezza dei dati nonché il rispetto e l'attivazione in caso di situazioni particolari come evidenziato nelle procedure "Procedura Data Breach" e "Procedura Esercizio Diritti Interessato Gelit".

Nel caso in cui si venga a conoscenza di dati personali e particolari di dipendenti, clienti e fornitori che non sono pertinenti per lo svolgimento delle proprie mansioni, è richiesta la massima riservatezza: tali informazioni devono essere eliminate dai sistemi informatici e/o dagli archivi cartacei della società e non devono essere in alcun modo divulgate sia all'interno che all'esterno della società.

Nel caso in cui si venga a conoscenza di dati personali e particolari di dipendenti, clienti e fornitori che sono raccolti in modo sovra-abbondante rispetto le finalità del trattamento, è richiesta la comunicazione al Titolare affinché lo stesso provveda a richiedere l'eliminazione della raccolta di tale dato.
Inoltre, se necessario, i Responsabili e il Titolare dovranno provvedere, a seguito di tale eliminazione, a modificare il registro dei trattamenti.