# GUIDA ALLE PRINCIPALI NOVITÀ DEL REGOLAMENTO EUROPEO SULLA PRIVACY


*Area lavoro e previdenza ver. 1.0*

CONFINDUSTRIA BERGAMO

# Indice

# 1. ENTRATA IN VIGORE ED EFFICACIA – A CHI E' RIVOLTO

Il Regolamento Europeo sulla privacy (2016/679/UE) è entrato in vigore il 24 maggio del 2016, ma la sua efficacia/applicabilità è differita in tutti i Paesi dell'Unione al 25 maggio 2018 (v. art. 99 del Regolamento).

Il nuovo GDPR, abroga espressamente la precedente direttiva 95/46/CE (art. 94 del Regolamento) sulla quale si fonda l'attuale Codice della privacy.

Il Regolamento si applica con riferimento ai dati personali (comuni, sensibili, biometrici, genetici ecc..) di persone fisiche[1], trattati da titolari o responsabili che si trovino all'interno dell'Unione europea o da parte di Titolari del trattamento che, pur trovandosi in ambito extra-Ue, offrano beni, prestino servizi o compiano attività di monitoraggio del comportamento di interessati che si trovino all'interno di uno degli Stati membri dell'Unione europea.

Si segnala, inoltre, che il Parlamento Italiano ha approvato in via definitiva il DDL di delegazione europea 2016. L'art. 13 del DDL contiene la delega al Governo - da esercitarsi in 6 mesi - per l'adeguamento del quadro normativo nazionale alle disposizioni del nuovo Regolamento. Tra i criteri di delega, si prevede:

- l'abrogazione delle disposizioni del Codice privacy incompatibili con quelle del Regolamento;

- la modifica del Codice privacy limitatamente a quanto necessario per dare attuazione alle disposizioni del Regolamento non direttamente applicabili;

- il coordinamento delle disposizioni vigenti in materia di protezione dei dati personali con quelle del Regolamento;

- la previsione, ove opportuno, del ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante privacy nell'ambito e per le finalità di cui al Regolamento;

- la previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni del Regolamento.

Al contrario di quanto previsto dalla legge delega, lo schema di decreto attuativo, in fase di promulgazione, prevede l'abrogazione totale del Codice della privacy, nonché:

- La facoltà per il Garante Italiano di poter emanare misure di semplificazione per le PMI;
- una disciplina transitoria volta ad assicurare il riordino, previa consultazione pubblica, delle autorizzazioni generali del Garante e ad indirizzare l'interpretazione dei Provvedimenti dell'Autorità e a definire in maniera rapida i procedimenti davanti alla stessa;
- la conferma del regime privacy previsto per i dati contenuti nei CV spontaneamente inviati;

[1] Non si applica ai dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto (v. *considerandum* 14). Non si applica nell'ambito di attività esclusivamente personali o di carattere domestico (v. *considerandum* 18).

## E i provvedimenti generali?

I provvedimenti generali emanati dal Garante Italiano (es. in materia di videosorveglianza, di geolocalizzazione, sul trattamento dei dati biometrici, sui cookie, spam, comunicazioni commerciali, amministratore di sistema ecc.) continueranno ad applicarsi anche dopo l'applicazione del GDPR.

E' comunque auspicabile aspettarsi una pronuncia da parte del Garante volta ad adeguare i vecchi provvedimenti con la nuova disciplina, posto che i riferimenti contenuti nei Provvedimenti Generali fanno rimando alla normativa dettata dal d.lgs. 196/03.

## 2. SOGGETTI DEL TRATTAMENTO

### a) Titolare del trattamento dei dati (artt. 4 e 24)

Come prevede l'articolo 4 del Regolamento il titolare del trattamento è 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 la 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.

Il titolare non deve essere nominato dal momento che la sua figura è già individuata dalla legge.

### b) Contitolare del trattamento (art. 26) NEW!!!

Il regolamento ammette espressamente la possibilità che un determinato trattamento sia effettuato da più titolari, allorché ne determinino congiuntamente finalità e mezzi.

Le responsabilità in merito all'osservanza degli obblighi previsti dal GDPR è ripartita dai contitolari attraverso un accordo interno che evidenzi i rispettivi ruoli nell'ambito del trattamento.

L'accordo deve prevedere dunque una ripartizione degli obblighi del Regolamento (es. esercizio dei diritti dell'interessato), le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del Regolamento. L'accordo, inoltre, deve essere messo a disposizione dell'interessato.

### c) Responsabile del trattamento

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

Deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate tali da garantire il rispetto delle prescrizioni del Regolamento e la tutela dei diritti dell'interessato.

Può essere nominato tramite:

- contratto;

- altro atto giuridico a norma del diritto dell'Unione Europea o degli Stati membri;

A differenza del passato la lettera di nomina (o il contratto) non può limitarsi ad una descrizione dei compiti e alle istruzioni per il trattamento, ma deve indicare specificatamente la materia, la durata, la natura e le finalità, la tipologia dei dati personali oggetto del trattamento, le categorie di interessati e gli obblighi e diritti del titolare. NEW!!!

Inoltre anche il responsabile ha, a sua volta, la possibilità di nominare un nuovo responsabile o un suo rappresentante. NEW!!!

*Responsabilità del responsabile:* il Responsabile risponde dell'illegittimo trattamento solo se non ha adempiuto agli obblighi previsti dal Regolamento a suo carico o se ha agito in maniera difforme rispetto alle istruzioni del titolare (resta co-obbligato con il titolare). E' esonerato da responsabilità solo se prova che il fatto non è a lui imputabile.

Vai al modello

## d) Persone autorizzate – incaricato del trattamento

Il Regolamento Europeo non prevede più la figura dell'incaricato del trattamento (art. 30 del Codice della privacy), ma non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Potrebbe essere opportuno, pertanto, continuare a nominare tale figura o, comunque, continuare a fornire istruzioni per iscritto alle persone autorizzate al trattamento dei dati, in quanto il Regolamento prevede espressamente un obbligo di istruire/formare il personale che tratta dati di carattere personale all'interno dell'azienda.

## e) Data protection officer – Responsabile per la protezione dei dati NEW!!!

In base al nuovo Regolamento Europeo alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO (interno o esterno[2]) in via obbligatoria.

Il DPO è una persona designata in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa (GDPR) e delle prassi nazionali ed europee, nonché della capacità di assolvere ai propri compiti (art. 37 GDPR).

Al DPO devono essere fornite le risorse necessarie per assolvere I compiti previsti dall'art. 39 del Regolamento e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Una volta nominato il DPO deve essere coinvolto in ogni questione riguardante la protezione dei dati personali.

In base all'articolo 37, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;

b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Per comprendere meglio quando sia necessario nominare un DPO è essenziale circoscrivere le definizioni di "attività principali", "larga scala" e "monitoraggio sistematico".

### Attività principali

Attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile → es. il trattamento dei dati relativi alla salute è da ritenersi attività principale di qualsiasi ospedale.

### Larga scala

È raccomandabile tener conto, per stabilire se un trattamento sia effettuato su larga scala, dei seguenti fattori:

[2] Mediante la stipula di un contratto di servizi.

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;

- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);

- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;

- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;

- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

### Monitoraggio regolare e sistematico

L'aggettivo regolare può significare:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;

- ricorrente o ripetuto a intervalli costanti;

- che avviene in modo costante o a intervalli periodici.

L'aggettivo sistematico può significare:

- che avviene per sistema;

- predeterminato, organizzato o metodico;

- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;

- svolto nell'ambito di una strategia.

Alcune esemplificazioni fornite dal Gruppo di lavoro sulla tutela delle persone fisiche (WP 29), in merito al concetto di monitoraggio regolare e sistematico:

- curare il funzionamento di una rete di telecomunicazioni;

- prestazione di servizi di telecomunicazioni;

- reindirizzamento dei messaggi di posta elettronica;

- profilazione e scoring per finalità di valutazione del rischio (es. ai fini di valutare il rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio);

- tracciamento dell'ubicazione, per esempio attraverso app su dispositivi mobili;

- programmi di fidelizzazione;

- pubblicità comportamentale;

- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;

- utilizzo di telecamere a circuito chiuso;

- dispositivi connessi quali contatori intelligenti, dispositivi di domotica ecc…

Vai al modello

## f) L'amministratore di sistema

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provv. gen. 27 novembre 2008 vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi.

L'amministratore di sistema ha il compito di predisporre le misure di sicurezza idonee a garantire la sicurezza e l'integrità dei dati trattati dal titolare che circolano attraverso sistemi informatici. Inoltre deve predisporre le misure minime di sicurezza previste dal Disciplinare Tecnico (all. B) del Codice della privacy e riassunte nella seguente tabella.

| **REGOLA ALL. B** | **COMPITI AMMINISTRATORE** |
|---|---|
| 1-11 | *Prevedere un sistema di autenticazione informatica e adottare le procedure per la gestione delle credenziali di autenticazione.*<br><br>- assegnare ad ogni incaricato una o più credenziali di autenticazione (codice identificativo personale e parola chiave, dispositivo di autenticazione o caratteristica biometrica), eventualmente associate tra loro; |

| | |
|---|---|
| | o il codice identificativo deve essere assegnato individualmente e non è riutilizzabile<br><br>- disattivare le credenziali in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali, nonché le credenziali non utilizzate da almeno 6 mesi. |
| 12-15 | L'ADS deve:<br><br>- individuare profili di autorizzazione di ambito diverso per ciascuno o per classi omogenee di incaricati;<br><br>- curare l'aggiornamento periodico, secondo le periodicità previste dalla legge, dei profili di autorizzazione degli incaricati e dell'ambito di trattamento consentito agli addetti alla gestione e manutenzione degli strumenti. |
| 16-17 | *Adottare misure per la protezione di strumenti e dati rispetto a trattamenti illeciti e accessi non consentiti.*<br><br>- attivare idonei strumenti elettronici per evitare intrusioni e l'azione di programmi diretti a danneggiare o interrompere un sistema informatico (antivirus);<br><br>- installare periodicamente gli aggiornamenti dei programmi per elaborare volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti (*patch* o programmi *update.* |
| 18, 20-23 | *Adottare procedure per la custodia di copie di sicureza, il ripristino della disponibilità dei dati e dei sistemi.*<br><br>- adottare idonee misure per garantire i ripristino dell'accesso ai dati sensibili o giudiziari in caso di danneggiamenti;<br><br>- proteggere i dati sensibili o giudiziari contro ogni accesso abusivo (*firewall)*<br><br>- predisporre misure che prevedano che i supporti rimovibili di memorizzazione di dati sensibili o giudiziari, laddove non vengano più utilizzati, siano distrutti o resi inutilizzabili ovvero riutilizzati da altri incaricati, nel solo caso in cui le informazioni precedentemente contenute non siano intelligibili o altrimenti ricostruibili; |
| 24 | *Adottare tecniche di cifratura per i trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.* |

# COSA CAMBIA? NOVITA' RISPETTO AL D.LGS. 196/03

## L'informativa (artt. 13 e 14 GDPR) NEW!!!

Come il Codice della privacy anche il Regolamento Europeo prescrive l'obbligo di fornire un'informativa all'interessato prima di effettuare la raccolta dei dati (art. 13 GDPR) o, se i dati non sono raccolti direttamente presso l'interessato (art. 14 GDPR) entro un termine ragionevole e, comunque, non oltre 1 mese dall'ottenimento dei dati, oppure al momento della comunicazione (non della registrazione) dei dati a terzi o all'interessato (diversamente a quanto prevede l'art. 13 c. 4 del Codice della privacy).

Il contenuto dell'informativa si arricchisce di ulteriori elementi obbligatori rispetto al passato. Oltre l'indicazione puntuale delle finalità del trattamento, l'esistenza di un responsabile del trattamento e i destinatari dei dati, l'obbligatorietà o meno del conferimento, l'indicazione dei diritti degli interessati[3], il titolare del trattamento deve, secondo la nuova normativa, fornire anche le seguenti informazioni: i dati di contatto del DPO (se nominato), la base giuridica del trattamento (ex art. 6 GDPR[4]), quale è il suo interesse legittimo (laddove questo costituisca la base giuridica del trattamento), nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (v. artt. 45, 46, 47, 49 GDPR[5]), il periodo di conservazione dei dati e il diritto di presentare un reclamo all'autorità di controllo, se il trattamento comporta processi decisionali automatizzati e se sono compiute attività di profilazione - indicando anche la logica di tali processi decisionale le conseguenze previste per l'interessato.

Vai al modello

## Base giuridica del trattamento- condizioni di liceità (art. 6 GDPR) NEW!!!

Anche il nuovo Regolamento prevede che ogni trattamento debba trovare fondamento in un'idonea base giuridica.

In particolare il trattamento è lecito se basato su consenso, o se compiuto per adempiere ad obblighi contrattuali, o per preservare interessi vitali della persona interessata o di terzi, per l'adempimento di obblighi di legge cui è soggetto il titolare, per finalità di pubblico interesse o per l'esercizio di pubblici poteri, o a fronte di un interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Per quanto attiene alla valutazione circa la prevalenza fra il legittimo interesse del titolare o del terzo e i diritti e le libertà dell'interessato si ritiene che questa debba essere effettuata direttamente al titolare, quale espressione del principio di *accountability (*responsabilizzazione) introdotto dal nuovo pacchetto protezione dati.

[3] Diritti che, tuttavia, subiscono un significativo ampiamento.
[4] V. par. successivo.
[5] Il riferimento è all'esistenza di una decisione di adeguatezza (cfr. art. 45 GDPR), o la presenza di garanzie adeguate (art. 46 GDPR) o di norme vincolanti d'impresa (*binding corporate rules* art. 47 GDPR), a decisioni di adeguatezza o alle deroghe specifiche espressamente previste per la salvaguardia di diritti e/o situazioni particolari (art. 49 GDPR).

L'applicazione del principio di bilanciamento di interessi non deve essere indiscriminata: nel caso l'interesse legittimo del titolare non fosse ritenuto prevalente, infatti, si potrebbe configurare il caso di un illecito trattamento con le conseguenze sanzionatorie previste dall'art. 83 c. 5 lett. A) del GDPR.

In caso di dubbi circa la prevalenza del suddetto interesse conviene, quindi, richiedere un consenso all'interessato.

Il consenso deve essere esplicito quando riferito a dati sensibili o per le decisioni basate su trattamenti autorizzati. E' consigliabile che questo venga prestato in "forma scritta", dal momento che grava sul titolare l'onere di dimostrare che l'interessato lo abbia effettivamente prestato.

In deroga a quanto previsto dall'art. 2 c.c., il Regolamento europeo prevede che la capacità d'agire in materia di riservatezza si acquista al compimento dei 16 anni; prima di tale età occorre raccogliere il consenso del minore da chi ne esercita la potestà[6].

## Misure di sicurezza (art. 32 GDPR) NEW!!!

Il nuovo Regolamento Europeo non stabilisce nel dettaglio le misure di sicurezza da adottare da parte dell'azienda, limitandosi a stabilire dei parametri. In particolare "il titolare deve attivare le misure di sicurezza tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche".

Scompare, dunque, rispetto al Codice della privacy, il duplice riferimento alle misure idonee e misure minime, quest'ultime, descritte compiutamente nell'allegato tecnico (All. B).

E' bene, comunque continuare a predisporre le misure minime di sicurezza previste dal d.lgs. 196/03 posto che le stesse sono richiamate dal Provv. Generale 27 novembre 2008, quali misure necessariamente da predisporre da parte dell'Amministratore del sistema nominato.

## Valutazione d'impatto sulla protezione dei dati (art. 35 c.d privacy by design) NEW!!!

La valutazione d'impatto sulla protezione dei dati deve essere effettuata prima di iniziare un trattamento che preveda rischi elevati per i diritti e le libertà delle persone fisiche. Va eseguita necessariamente quando l'azienda tratti su larga scala dati sensibili, biometrici, genetici, giudiziari, oppure faccia attività di profilazione; o svolga attività di sorveglianza sistematica su larga scala di una zona accessibile al pubblico. La valutazione deve contenere:

a) una descrizione sistematica dei trattamenti e delle finalità del trattamento;

[6] Ciò significa ad esempio che l'informativa deve essere consegnata direttamente al minore e il consenso da lui direttamente prestato.

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà dell'interessato;

d) le misure previste per affrontare i rischi e le misure di protezione dei dati.

Le linee guida del 4 aprile 2017, così come modificate in data 4 ottobre dall'autorità Garante, prevedono inoltre l'obbligo di effettuare la VIP qualora il trattamento integri almeno 2 dei seguenti criteri:

1. Trattamento che riguardi aspetti quali "*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*";
2. Processi decisionali automatizzati che hanno effetti giuridici o che incidono in modo analogo sulle persone;
3. Monitoraggio sistematico;
4. Dati sensibili o dati aventi carattere altamente personale;
5. Trattamenti su larga scala;
6. Creazioni di corrispondenze o combinazione di insiemi di dati;
7. Dati relativi a interessati vulnerabili;
8. uso innovativo od applicazione di nuove soluzioni tecnologiche od organizzative;
9. quando il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Vai al modello

## Consultazione preventiva all'autorità Garante (art. 36) NEW!!!

Con il nuovo Regolamento Europeo scompare l'istituto della notifica preliminare al Garante, obbligatoria secondo il d.lgs. 196/03 per determinati trattamenti. Si assiste ad una inversione di rotta, dal momento che il Regolamento prevede che la consultazione preventiva all'autorità Garante sia effettuata solo laddove, all'esito della procedura d'impatto sulla protezione dei dati, si ritiene che il trattamento possa presentare un rischio elevato in assenza di misure di sicurezza attuate dal titolare per attenuarne il rischio.

In particolare, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 del Regolamento Europeo;

f) ogni altra informazione richiesta dall'autorità di controllo.

## Data breach (violazione dati personali – artt. 33 e 34) NEW!!!

In caso di violazione dei dati personali il titolare del trattamento deve notificare la violazione all'autorità di controllo competente a norma dell'art. 55 (Garante Italiano) senza ingiustificato ritardo e, ove possibile, entro 72h dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Il titolare dovrà specificare i motivi del ritardo qualora la notificazione avvenga oltre le 72h. Se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Il titolare del Trattamento dovrà, inoltre comunicare agli interessati quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

## Codici di condotta (artt. 24 c. 3 e 40) NEW!!!

Il Regolamento Europeo prevede che l'impresa possa aderire ad un codice di condotta elaborato da associazioni o da altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento.

L'adesione al codice di condotta può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

## Certificazione (art. 42 e ss.) NEW!!!

Il titolare può richiedere la certificazione di conformità al Regolamento di determinati trattamenti.

Ancora non sono presenti meccanismi di certificazione in Italia.

## Principi privacy - Privacy by default - principio di non eccedenza (art. 5 lett. c e art. 6)

L'art. 5 del Regolamento Europeo prescrive che il trattamento dei dati debba essere effettuato seguendo determinati principi. In particolari i dati devono essere:

- raccolti per finalità determinate esplicite e legittime;

- adeguati pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

- esatti e, se necessario, aggiornati, nonché devono essere adottate misure ragionevoli per cancellare e rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza).

- conservati per un lasso di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

- trattati in maniera da garantire un'adeguata sicurezza dei dati personali

## Registro attività di trattamento (art. 30 GDPR) NEW!!!

I titolari (e i responsabili) di aziende con più di 250 dipendenti o che trattino dati sensibili o giudiziari, devono tenere un registro dei trattamenti che deve indicare:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative;

Anche il responsabile del trattamento è tenuto a tenere un proprio registro del trattamento nel quale sono contenute

Il responsabile del trattamento tenuto alla redazione di un registro di trattamenti deve indicare nello stesso:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del

trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Vai al modello

# 4. IL TRATTAMENTO DEI DATI ALL'INTERNO DELL'AZIENDA

## I dati dei lavoratori dipendenti

Come è noto, il trattamento dei dati delle persone fisiche deve essere necessariamente effettuato secondo quanto previsto dalla normativa privacy vigente. Non fa eccezione il trattamento dei dati personali effettuato dal datore di lavoro nei confronti dei propri lavoratori dipendenti.

Con la Deliberazione n. 53 del 23 novembre 2006 il Garante è intervenuto sulla materia disponendo delle linee guida per il trattamento dei dati dei lavoratori dipendenti.

Con i necessari adattamenti è possibile ritenere, almeno fino a nuove disposizioni, che gli indirizzi contenuti nelle suddette linee guida siano ancora da seguire.

In particolare:

- il datore di lavoro è tenuto a rendere al lavoratore, prima di procedere al trattamento dei dati personali che lo riguardano un'informativa individualizzata (artt. 13 e 14 Reg. EU.); → v. modello allegato

- il datore di lavoro è tenuto ad ottenere il previo consenso del lavoratore qualora:

a) utilizzi per finalità particolari i dati (es. trattamento di dati genetici, biometrici ecc…);
b) comunichi i dati ad altri soggetti per i quali la legge non prevede adempimenti obbligatori (es. associazione datoriali);

Al contrario, il consenso non è richiesto e, quindi, il trattamento è lecito quando:

- è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- È necessario per adempiere ad obblighi di legge;
- È necessario per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica;
- 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;
- Il trattamento è necessario per il perseguimento di un legittimo interesse del titolare del trattamento o di terzi.

## Semplificazioni nel trattamento dei dati per finalità di marketing diretto e la profilazione

Come già accennato, la nuova disciplina si fonda sul principio di "*accountability*". Questa nuova impostazione consente alle aziende di snellire numerosi adempimenti che sono, invece, prescritti dalla normativa "Codicistica" (d.lgs. 196/03).

Segnatamente, per quanto attiene alla finalità di marketing diretto il codice della privacy prevede l'obbligo, in capo al titolare del trattamento, di fornire l'informativa all'interessato e di ottenere dallo stesso un idoneo consenso.

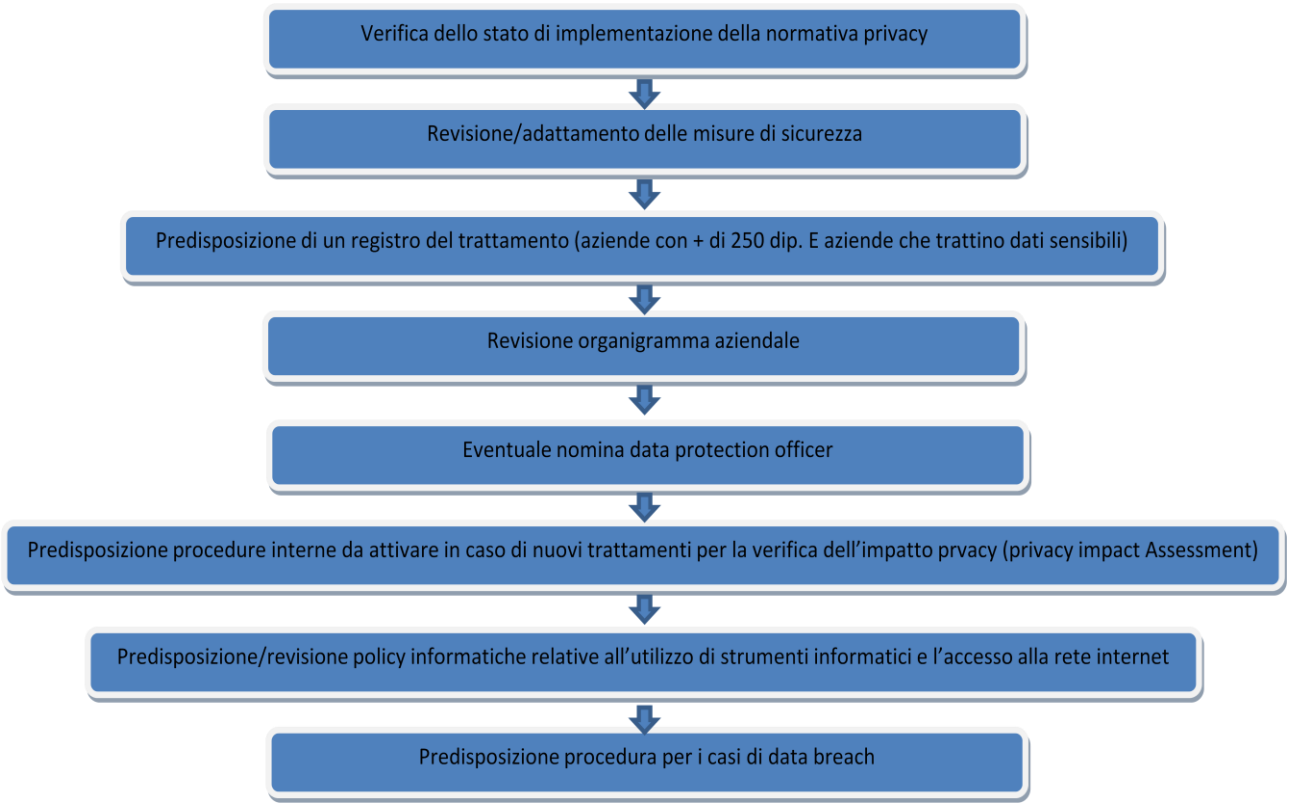
Con il Regolamento Europeo l'obbligo di ottenere un consenso scompare, laddove la base giuridica del trattamento, da indicare necessariamente nell'informativa, è rappresentata dal legittimo interesse del titolare.

Semplificazioni sono poi introdotte per quanto attiene al trattamento di dati personali attraverso la loro profilazione. Nella vigenza del Codice della privacy il Titolare del trattamento, oltre al rilascio dell'informativa e alla richiesta del consenso doveva altresì, effettuare la notifica preliminare del trattamento al Garante.

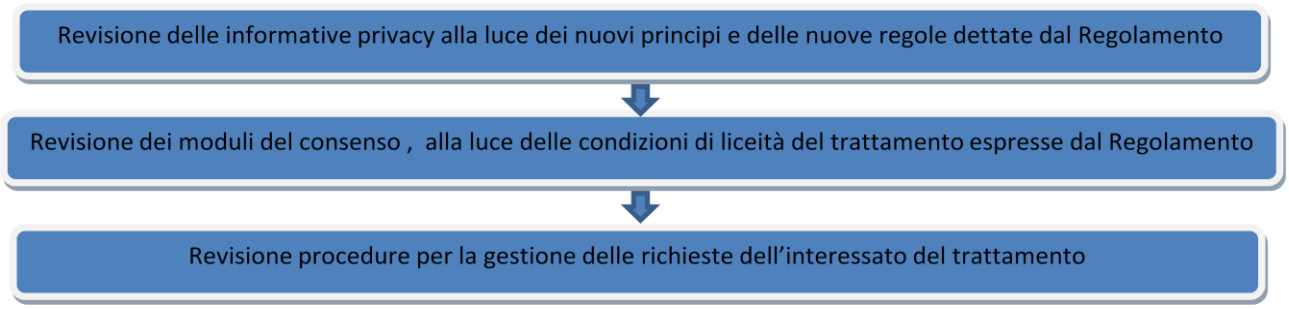
Con il Regolamento Europeo, attraverso il principio di autoresponsabilizzazione del Titolare, pur permanendo la necessità di rivolgere l'informativa all'interessato ed ottenere un valido consenso, non è più necessario, invece, effettuare alcuna notifica al Garante (salvo che il Trattamento, all'esito della valutazione del rischio, possa comportare rischi particolari per i dati dell'interessato).

## 5. In sintesi: cosa fare per adeguare il proprio trattamento al regolamento

All'interno dell'azienda:



Nei rapporti con gli interessati:




Nei rapporti con fornitori di servizi/destinatari di dati:

# 5) MODULISTICA (fac-simili)

## 1) Contratto di nomina a responsabile del trattamento

*Il testo che segue rappresenta una bozza per la redazione della nomina a responsabile del trattamento, essa dovrà pertanto essere adattata in relazione alla specifica realtà organizzativa ed operativa dell'impresa.*

*(da redigere su carta intestata della società )*

CONTRATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO

ai sensi del Regolamento Europeo per la protezione dei dati (Reg. UE. 2016/679)

tra

La società …… con sede in ……, in persona del legale rappresentante pro tempore, Titolare, ai sensi dell'art. 4 comma 1 n. 7), del Reg. UE 2016/679, del trattamento dei dati personali di utilizzo attuale o futuro da parte della suddetta persona giuridica,

e

la società _____, C.F. _____nato/a / a _____, in qualità di _____;

premesso che

- la società _____ ha incaricato la società _____ di _____

- che tale operazione comporta e realizza a tutti gli effetti un trattamento dei dati personali ai sensi della normativa privacy;

si conviene

In applicazione delle disposizioni di cui all'art. 28, del Reg. UE. 2016/679, l'intestata società affida al sig./alla società _____ l'incarico di **responsabile del trattamento.**

L'incarico conferito di responsabile del trattamento ha lo scopo di garantire una gestione maggiormente oculata del flusso di dati personali trattati.

Detto incarico durerà_____ (es. *per il tempo strettamente necessario ad assolvere alle finalità di cui in premessa ed in ogni caso per un tempo non superiore alla durata del contratto di manutenzione*).

Durante lo svolgimento di detto incarico, il responsabile potrà venire a conoscenza - e di conseguenza dovrà trattare e garantire la riservatezza - di dati personali di natura comune e sensibile (ivi compresi dati di carattere giudiziario, biometrico e genetico nonché dati relativi alla salute delle persone) riferiti, in particolare ai lavoratori dipendenti dell'azienda, a clienti e fornitori (anche solo potenziali) di beni e servizi.

Il "Responsabile del trattamento dei dati" dichiara di essere a conoscenza di quanto stabilito dal Reg. 2016/679/UE e si impegna, pertanto, ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte ed, in particolar modo, rispetto a quanto stabilito dall'art. 28 del citato Regolamento.

Il "Responsabile del trattamento dei dati" dovrà curare i seguenti adempimenti:

- garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare le misure di sicurezza ai sensi dell'art. 32;
- non ricorrere ad altro responsabile del trattamento se non previa autorizzazione scritta del titolare del trattamento;
- garantire il rispetto degli obblighi in materia di sicurezza nonché di consultazione preventiva qualora la valutazione d'impatto sulla protezione dei dati indichi che uno specifico trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
- cancellare o restituire tutti i dati personali nel momento in cui è terminata la prestazione dei servizi relativi al trattamento e cancellare altresì le copie esistenti salvo che per quel trattamento sia prevista la conservazione dei dati;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei suddetti obblighi, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.
- Informare il titolare del trattamento qualora, un'istruzione violi la normativa in materia di protezione dei dati personali.
- Redigere e tenere aggiornato un registro delle attività di trattamento, contenente le informazioni prescritte dall'art. 30 del Reg. 2016/679/UE;
- Mettere a disposizione il Registro del trattamento all'autorità di controllo;
- comunicare al Titolare, la descrizione delle modalità tecnico-organizzative del trattamento (nonché ogni mutamento nelle stesse), con particolare riferimento alle misure adottate per garantire riservatezza e integrità dei dati;
- attuare gli obblighi di informazione e di acquisizione del consenso verificando scrupolosamente le singole fattispecie in modo da garantire la regolare esecuzione delle procedure previste dagli articoli di legge che regolamentano tali obblighi;
- garantire agli interessati l'effettivo esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21, *Reg (UE) 2016/679,* ivi compreso il diritto di proporre reclamo a un'autorità di controllo, sul trattamento dei loro dati adempiendo ai corrispettivi obblighi, accertandosi anche che ogni modulo di informativa sottoposto agli interessati contenga - in allegato – dette previsioni;
- vigilare sul rispetto delle misure di sicurezza da parte dei soggetti autorizzati al trattamento;
- una volta terminato il trattamento, restituire al Titolare - nel rispetto della normativa vigente - tutte le informazioni che costituiscono le Banche Dati oggetto del trattamento e a distruggere tutte le copie dei dati presenti in qualsiasi forma (cartacea, magnetica, ecc.);
- ogni incombenza comunque connessa all'esecuzione dell'incarico in questione e necessaria/opportuna per l'esercizio dei compiti riportati nella presente, attribuendogli pertanto il potere di adottare in piena autonomia tutte le iniziative e gli interventi idonei a garantire il corretto esperimento della funzione affidata nel rispetto delle statuizioni della normativa vigente in materia di protezione dei dati personali.

Il responsabile del trattamento dovrà, inoltre, coadiuvare il Titolare del trattamento nell'assolvimento degli obblighi e nell'esercizio dei diritti attribuiti al medesimo dal Regolamento 679/2016/UE. In particolare si rammenta che, ai sensi del Regolamento 679/2016/UE, il Titolare dovrà:

1. Mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento 679/2016/UE;
2. Attuare politiche adeguate in materia di protezione dei dati;
3. Mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Dette misure devono garantire, altresì, la conservazione dei dati per un periodo congruo e l'accessibilità da parte dei soli soggetti interessati; la pseudonominizzazione e la minimizzazione dei dati;

4. Notificare le violazione dei dati (*c.d. data breach*) all'autorità di controllo e comunicare la violazione all'interessato nel rispetto dei termini e delle modalità previste dagli artt. 33 e 34 del Regolamento 679/2016/UE;
5. Nei rapporti con gli interessati, dare un'idonea informativa e verificare a quali condizioni può trattare i dati e rispettare le condizioni di liceità del trattamento;

Quanto sopra fermo restando l'obbligo a carico del/della Sig./Sig.ra/della società …….. di operare secondo le istruzioni generali impartite dal titolare;

Si rappresenta che, ai sensi dell'art. 28, comma 10 del Reg. 679/2016/UE, qualora il Responsabile violi le disposizioni in materia di riservatezza dei dati personali, determinando finalità e mezzi del trattamento in violazione del citato Regolamento, questo è considerato un titolare del trattamento in questione.

Per tutto quanto non previsto nel presente atto si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

(Luogo e data)

Il Titolare del trattamento dei dati

Il Responsabile del trattamento dei dati

## 2) Contratto di affidamento incarico di responsabile per la protezione dei dati

*(da redigere su carta intestata della società )*

CONTRATTO DI AFFIDAMENTO INCARICO DI RESPONSABILE PER LA PROTEZIONE DEI DATI[7]

ai sensi del Regolamento Europeo per la protezione dei dati (Reg. UE. 2016/679)

tra

La società …… con sede in ……, in persona del legale rappresentante pro tempore, Titolare[1], ai sensi dell'art. 4 comma 1 n. 7), del Reg. UE 2016/679, del trattamento[2] dei dati personali[3] di utilizzo attuale o futuro da parte della suddetta persona giuridica,

e

il sig./la sig.ra _____, C.F./P.IVA _____nato/a a _____, in qualità di _____[8];

In applicazione delle disposizioni di cui all'art. 37, del Reg. UE. 2016/679, l'intestata società affida al sig. _____, anche in ragione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione di dati, e della capacità di assolvere i compiti di cui all'articolo 39, come di seguito meglio dettagliati, l'incarico di **responsabile della protezione dei dati (di seguito RPD/DPO).**

1. OBBLIGHI E DIRITTI DEL TITOLARE DEL TRATTAMENTO

Nell'ambito del presente contratto il Titolare del trattamento e il responsabile del trattamento da questi nominato hanno l'onere di:

a. pubblicare i dati di contatto del RPD e comunicarli all'autorità di controllo;

b. fornire al RPD le risorse necessarie per consentirgli di: assolvere i compiti di cui all'articolo 39, garantire l'accesso ai dati personali e ai trattamenti, mantenere la propria conoscenza specialistica

c. garantire l'indipendenza del RPD assicurandosi che non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti.

Il responsabile e il Titolare del trattamento potranno attribuire al RPD altri compiti e funzioni, purché non generino conflitto d'interesse con la sua carica;

2. OBBLIGHI E DIRITTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

In qualità di responsabile della protezione dei dati lei dovrà:

[7] In base all'articolo 37, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:
a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.
Per ulteriori approfondimenti in argomento v. Linee guida sul data protection officer del WP29 del 16.12.2016.

[8] Specificare se dipendente del titolare del trattamento, del responsabile del trattamento, o se consulente esterno della Società [*indicare ragione sociale e recapiti della società*].

a. rispondere agli interessati che potranno contattarla per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Regolamento;

b. riferire direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

c. mantenere il segreto e la riservatezza in merito all'adempimento dei suoi compiti, in conformità con il diritto dell'Unione europea o degli Stati membri;

d. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguano il trattamento in merito agli obblighi derivanti dal regolamento 679/2016/UE, nonché da altre disposizioni normative e/o provvedimenti generali in materia di protezione dei dati;

e. sorvegliare l'osservanza della normativa vigente in materia di protezione dei dati personali nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione di dati personali, compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

f. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare lo svolgimento ai sensi dell'articolo 35 del Regolamento 679/2016/UE.

g. cooperare con l'autorità di controllo (il Garante per la protezione dei dati)e fungere da punto di contatto con quest'ultima per questioni connesse al trattamento, tra cui la consultazione preventiva ex art. 36 del Regolamento 679/2016/UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

h. considerare i rischi connessi al trattamento nello svolgimento dei suoi compiti, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

3. DURATA DEL CONTRATTO

Il presente contratto ha durata _____ e sarà rinnovato tacitamente per un ulteriore periodo di _____ alla scadenza.

Al fine di evitare il suddetto rinnovo le parti dovranno presentare formale disdetta alla controparte almeno _____gg. prima della scadenza.

4. COMPENSO

Le parti concordano che, per l'intera durata del contratto, sarà corrisposta, in favore del RPD, una somma dell'importo di €_____. Tale somma verrà corrisposta con le seguenti modalità _____[9].

5. RISOLUZIONE DEL CONTRATTO

In caso di inadempimento degli obblighi previsti ai precedenti punti le parti potranno risolvere unilateralmente il presente contratto.

[9] Es. Integralmente all'atto di stipula del presente contratto/per metà alla stipula del contratto e la restante parte alla scadenza dello stesso.

[eventuale] In tal caso la parte inadempiente sarà tenuta al versamento di una penale quantificata in € _____, fatta salva la dimostrazione dell'eventuale danno ulteriore.

Per tutto quanto non previsto nel presente atto si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Luogo e data

IL TITOLARE DEL TRATTAMENTO

_____

IL R.P.D.

_____

## 3) Informativa privacy generale ex artt. 13 e 14 GDPR e consenso al trattamento

*L'informativa dovrà essere rilasciata all'interessato [10]:*
*a) al momento della raccolta dei dati presso l'interessato, nel momento in cui i dati personali sono ottenuti (art.13 Reg (UE) 2016/679);*
*b) se i dati personali non sono raccolti presso l'interessato, entro:*
*- un termine ragionevole dall'ottenimento dei dati, ma al più tardi entro un mese;*
*- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;*
*- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali (art. 14 num. 3 Reg (UE) 2016/679) .*
*Il testo qui riportato rappresenta semplicemente una bozza per la redazione dell'informativa che dovrà essere fornita ai dipendenti e pertanto dovrà essere adattata alla realtà organizzativa ed operativa della singola impresa.*
---

*(Redigere su carta intestata della società)*

Egr. Sig. / Gent.ma Sig.ra

.....

Oggetto: informativa resa all'interessato per il trattamento[11] dei dati personali comuni e sensibili[12]

Ai sensi degli artt. 13 e 14 *Reg (UE) 2016/679*, ed in relazione ai dati personali che si intendono trattare, La informiamo di quanto segue:

1. il trattamento a cui saranno sottoposti i dati personali sarà effettuato al fine di _____; base giuridica del trattamento è _____[13];
2. il trattamento è effettuato nel rispetto dei principi e delle modalità previste dal *Regolamento 2016/679/UE*, in particolare degli artt. 5 e 6 e 22[14], comprenderà tutte le operazioni o complesso di operazioni previste all'art.4 num. 2), *Regolamento 2016/679/UE*, necessarie al trattamento in questione, ivi inclusa la comunicazione nei confronti dei soggetti di cui al successivo punto 5), nonché la diffusione

[10] ex art.4 num 1), Reg (UE) 2016/679, "interessato": la 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

[11] ex art.4 num 2) Reg (UE) 2016/679, "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;

[12] ex art.4 num 1) Reg (UE) 2016/679, "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;

[13] indicare se il trattamento è basato: 1) sul consenso, 2) se compiuto per adempiere ad obblighi contrattuali, 3) o per preservare interessi vitali della persona interessata o di terzi, 4) per l'adempimento di obblighi di legge cui è soggetto il titolare, 5) per finalità di pubblico interesse o per l'esercizio di pubblici poteri, 6) su un interesse legittimo del titolare rispetto al diritto dell'interessato;

[14] citare tale articolo solo se il trattamento è effettuato attraverso processi decisionali automatizzati o che ne comportano la profilazione. In tal caso è necessario fornire informazioni circa la logica utilizzata, nonché L'importanza e le conseguenze previste per l'interessato.

nell'ambito richiamato al punto 7) della presente informativa; il trattamento avviene nel modo seguente:……[15];

3. il conferimento dei dati personali relativi al trattamento in parola ha natura _____ *(indicare se il conferimento deriva da un obbligo contrattuale, legale o se è un requisito necessario per la conclusione del contratto)*;
4. l'eventuale, parziale o totale, rifiuto di rispondere comporterà _____ *(indicare le conseguenze)* [16];
5. i dati personali relativi al trattamento in questione, per le finalità di cui al punto 1), verranno comunicati a _____[17];
6. dei dati forniti potranno venire a conoscenza le persone nominate responsabili del trattamento[18] o incaricate dall'azienda al trattamento e comunque ogni persona autorizzata al trattamento dal Titolare;
7. i dati personali in questione potranno/non potranno essere diffusi *(specificare l'ambito di diffusione, per es. nell'ambito dello Stato italiano)* e trasferiti all'estero ….. (specificare se il Paese terzo indicato ha ricevuto una decisione di adeguatezza dalla Commissione europea[19] o, in caso contrario, se si utilizzano BCR[20] di gruppo ove trasferiti all'interno di gruppi di imprese oppure se sono state inserite specifiche clausole contrattuali modello) *specificare se all'interno della UE o meno e gli Stati di destinazione, nonché l'esistenza o meno di una decisione di adeguatezza in caso di trasferimento ex artt. 46, 47 e 49 c.2 Reg (UE) 2016/679, il riferimento alle garanzie appropriate e opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono resi disponibili)*;
8. I dati personali in questione potranno saranno conservati per il tempo strettamente necessario ad assolvere alle finalità di cui al punto 1 ed, in ogni caso, per un periodo non superiore a _____anni.
9. all'interessato dal trattamento in esame è riconosciuto l'esercizio dei diritti di cui agli artt. 15, 16, 17, 18, 20, 21, *Reg (UE) 2016/679,* il cui testo integrale è riportato in allegato, ivi compreso il diritto di proporre reclamo a un'autorità di controllo;
10. titolare[21] del trattamento in parola è la società _____ *In persona del legale rappresentante pro tempore;* Responsabile del trattamento è il sig. _____ ; Responsabile per la protezione dei

---

[15] Per esempio:
- il trattamento è effettuato con o senza l'utilizzo di strumenti elettronici e gestito da personale appositamente incaricato;
- la conservazione dei dati avverrà in forma cartacea e/o su supporto magnetico/ informatico/ottico;
- i trattamenti di tipo manuale con raccolta dei dati medesimi su appositi registri e/o schede la cui conservazione sarà attuata con archiviazione tradizionale in appositi contenitori.

[16] Per esempio:l'impossibilità di perseguire in tutto o in parte le finalità indicate al punto 1);

[17] Indicare gli eventuali destinatari o le categorie dei soggetti ai quali possono essere comunicati i dati personali. Si richiamano qui di seguito, a titolo esemplificativo:
- alle pubbliche amministrazioni, con i criteri e nei limiti stabiliti dalla normativa vigente;
- alle organizzazioni sindacali dei lavoratori per gli adempimenti conseguenti all'attuazione delle trattenute sindacali;
- ai fondi o casse di previdenza e assistenza, al fine di …….. (per es.; iscrizione, gestione del conto individuale);
- alla Società ……..: ai fini della riscossione del premio relativo alla polizza ……..;
- alla Società ……..: ai fini della gestione del servizio paghe e contributi;
- al personale di Società esterne addette alla gestione e manutenzione dei sistemi informatici;
- ai rappresentanti dei lavoratori per la sicurezza quando gli stessi esercitino il diritto di accesso previsto dall'art. 50, comma 5, del D.Lgs. 81/2008;
- all'Organismo Paritetico Provinciale, relativamente al nominativo del Rappresentante dei Lavoratori per la Sicurezza;
- alle organizzazioni e/o alle aziende appartenenti al sistema Confindustria (con riguardo al personale dirigente avente eventuali incarichi sindacali in organismi delle associazioni dei datori di lavoro), a scopo informativo e per lo svolgimento dell'incarico;
- ad altre società facenti parte del gruppo, al fine di scambio di servizi e prestazioni tra le Società stesse;
- alle A.P.L. e società di formazione, per attività di formazione e/o supporto agli inserimenti al lavoro;
ecc.

[18] ex art.4 num 8), Reg (UE) 2016/679 «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;

[19] E' possibile verificare quali Paesi hanno ricevuto una decisione di adeguatezza consultando http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1;

[20] Bcr è l'acronimo di "binding corporate rules" ovvero regole vincolanti infragruppo che offrano pari garanzia di tutela dei dati rispetto alla normativa comunitaria.

[21] ex art.4 num 7), Reg (UE) 2016/679, «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;

dati[22] è il sig. _____ *(precisare gli estremi identificativi del titolare e, laddove nominato del responsabile, nonché del responsabile per la protezione dei dati[23], precisando le modalità per reperire il nominativo aggiornato del responsabile, i dati di contatto del medesimo. Se è stato designato un responsabile per il riscontro all'interessato, è indicato tale responsabile.)*.

……. lì ……..

Timbro e firma del legale rappresentante

Per ricevuta

……

Firma del lavoratore

All.: Art. 15, 16, 17, 18, 20, 21 *Reg (UE) 2016/679*

[22] Responsabile della porotezione dei dati - art. 37 Reg (UE) 2016/679

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5.Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

[23] È necessario nominare un responsabile per la protezione dei dati ogni qualvolta l'attività principale del titolare del trattamento (o del responsabile) consistano nel trattamento, su larga scala , di categorie particolari di dati personali di cui all'articolo 9 (dati sensibili, es. tessere sindacali) o di dati relativi a condanne penali e reati di cui all'art. 10, nonché qualora il trattamento richieda il monitoraggio regolare e sistematico degli interessati su larga scala.

## 4) Elenco dei diritti dell'interessato

*L'elenco sottostante di diritti dell'interessato è da riportare in calce ad ogni informativa.*

*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.

Sezione 3 **Rettifica e cancellazione**

*Articolo 16* **Diritto di rettifica**

1. 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 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.

Sezione 4 **Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche**

*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.

## 5) Fac- simile di consenso al trattamento dei dati personali del lavoratore (da aggiungere in calce all'informativa se il trattamento è fondato, in tutto o in parte, sul consenso)

Spett.le

_____

**Oggetto: consenso al trattamento dei miei dati personali**

Io sottoscritto _____, preso atto dell'informativa ex artt. 13 e 14, Reg. 679/2016/UE ed avuta integrale conoscenza delle informazioni in esso contenute, nonché dei diritti a me riconosciuti dagli artt. 15, 16, 17, 18, 20, 21, *Reg. 2016/679/UE,* ivi compreso il diritto di proporre reclamo a un'autorità di controllo, do atto che il trattamento è necessario per l'esecuzione del contratto di lavoro e, per quanto attiene ai seguenti specifici trattamenti:

- con riguardo al trattamento dei miei dati sensibili per le finalità indicate al punto 1 della menzionata informativa:

[ ] do il consenso [ ] nego il consenso

- con riguardo al trasferimento dei miei dati, anche sensibili, verso Paesi esteri o organizzazioni internazionali ex art. 44 e ss:[24]

[ ] do il consenso dichiaro di essere stato informato dei rischi derivanti da siffatto trasferimento, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate

[ ] nego il consenso

- con riguardo all'attività di profilazione dei miei dati o alle decisioni su di essi prese attraverso processi automatizzati, ex art. 22 del Reg. 2016/679/UE[25]

[ ] do il consenso [ ] nego il consenso

[24] da inserire solo nel caso in cui i dati siano trasferiti verso Paesi esteri che non abbiano ricevuto una decisione di adeguatezza, o qualora, nell'ambito di trasferimenti di dati infragruppo, nei rapporti con l'azienda ricevente situata nel Paese estero non siano stipulate delle norme vincolanti d'impresa (BCR). Se il trasferimento avviene in un Paese estero che ha ricevuto una decisione di adeguatezza non è necessario il consenso.

[25] Consenso da inserire solo nel caso in cui vengano effettuate attività di profilazione dei dati del lavoratore dipendente;

## 6) Valutazione d'impatto sulla protezione dei dati

La valutazione d'impatto è richiesta, preventivamente all'inizio del trattamento, qualora un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche[26].

TRATTAMENTO 1)

A) DESCRIZIONE DEL TRATTAMENTO E FINALITA' DELLO STESSO E INTERESSE LEGITTIMO PERSEGUITO DAL TITOLARE

_____
_____
_____
_____
_____
_____
_____
_____

B) VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO IN BASE ALLA FINALITA' PERSEGUITA

_____
_____
_____
_____
_____
_____
_____
_____

C) VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

_____
_____

[26] In particolare è richiesta in caso: a) qualora il trattamento consista in un valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, riguardi categorie particolari di dati personali di cui all'articolo 9 paragrafo 1 (dati sensibili, biometrici, genetici), oppure relativi a condanne penali e a reati di cui all'articolo 10; c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;

_____
_____
_____
_____
_____
_____

D) INDICAZIONE DELLE MISURE DI SIRCUREZZA PREVISTE PER AFFRONTARE I RISCHI

_____
_____
_____
_____
_____
_____
_____
_____

## 7) Registro trattamenti del Titolare/Responsabile del trattamento

## Registro trattamenti del Titolare/Responsabile del trattamento

*La compilazione di un registro del trattamento è obbligatoria solo per le imprese od organizzazioni con più di 250 dipendenti, oppure dal titolare che effettui trattamenti che possono presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o all'orientamento sessuale della persona, o i dati personali relativi a condanne penali o reati.*

*Il fac-simile sotto riportato rappresenta un esempio di registro del trattamento che può essere completato attraverso gli identificativi riportati nelle tabelle sottostanti (il contenuto di queste ultime deve, a loro volta, essere personalizzato in base al contesto aziendale di riferimento).*

FAC-SIMILE REGISTRO DEI TRATTAMENTI TITOLARE/RESPONSABILE DEL TRATTAMENTO

Nome del titolare/responsabile del trattamento[27]: _____

Nome del rappresentante del responsabile del trattamento[28]: _____

Data protection officer[29]: _____

| Tipo di trattamento e Finalità | Categorie di interessati | Categorie di dati personali | Categorie di destinatari a cui i dati sono comunicati | Trasferimento a Paese terzo (si no) ed eventuale indicazione del Paese o dell'Organizzazione internazionale | Termine per la conservazione / cancellazione | Descrizione Misure di sicurezza e organizzative |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

Esempio:

Finalità:

| *Identificativo* | *Descrizione finalità* |
|---|---|
| **1** | **Trattamento giuridico ed economico dei dati del personale (calcolo e pagamento retribuzioni ed emolumenti vari, applicazione della legge previdenziale ed assistenziale, ricorso ad ammortizzatori sociali)** |
| A | Gestione paghe |
| B | Tessere sindacali |
| C | Comunicazioni uso ammortizzatori INPS o MINISTERO LAVORO |

[27] Inserire solo se il registro è compilato da un responsabile del trattamento nominato dall'azienda.
[28] Indicare se nominato il rappresentante del responsabile del trattamento.
[29] Indicare se nominato il nome del responsabile della protezione dei dati (DPO);

| | |
|---|---|
| D | Inoltro a INPS |
| E | Inoltro a INAIL |
| **2** | **Igiene e sicurezza sul lavoro** |
| **3** | **Gestione della clientela persone fisiche** |
| **4** | **Gestione controversie (giudiziali e stragiudiziali)** |
| **5** | **Strumenti di controllo a distanza** |
| A | Badge aziendale/registratore presenze |
| B | Videosorveglianza |
| C | geolocalizzazione |
| … | |

Categorie di interessati:

| *Identificativo* | *Descrizione interessati* |
|---|---|
| i1 | Personale e loro familiari |
| i2 | Clienti persone fisiche |
| i3 | Potenziali clienti persone fisiche |
| i4 | Potenziali dipendenti/collaboratori |
| … | |

Categorie di dati personali

| *Identificativo* | *Descrizione dato trattato* |
|---|---|
| **c** | **Dato comune** |
| **s** | **Dato sensibile** |
| **g** | **Dato giudiziario** |
| … | |

Categorie di destinatari a cui sono comunicati i dati:

| *Identificativo* | *Destinatario* |
|---|---|
| d1 | Ufficio paghe |
| d2 | Associazioni datoriali e sindacati |
| d3 | Enti previdenziali e assistenziali |
| d4 | Autorità giudiziaria e altri |
| d5 | Autorità di pubblica sicurezza |
| d6 | Società di manutenzione |
| d7 | Medico competente |
| d8 | Responsabili e incaricati azienda |
| … | |

Descrizione Misure di sicurezza e organizzative

| *Identificativo* | *Destinatario* |
|---|---|
| S1 | Protezione attraverso password di almeno 8 caratteri con almeno 1 lettera maiuscola e 1 numero, modificata ogni 3 mesi; |

| | |
|---|---|
| S2 | Accesso tramite badge o altro dispositivo; |
| S3 | Disabilitazione automatica credenziale dopo 3 tentativi di accesso non andati a buon esito; |
| S4 | Firewall e antivirus presenti e aggiornati almeno ogni 6 mesi; |
| S5 | Registrazione degli accessi in file di log; |
| S6 | Disabilitazione utente in caso inattivo da almeno 6 mesi; |
| S7 | Procedura di backup dei dati con cadenza settimanale in server remoto e/o tramite sistemi cloud; |
| S8 | Compartimentazione dei dati: i dati sono accessibili solo alle aree aziendali interessate; |
| S9 | Scansione antivirus automatica della rete e singoli pc mensile; |
| S10 | Continuità dell'alimentazione elettrica garantita attraverso un sistema di alimentazione d'emergenza; |
| S11 | Il locale o l'armadio contenente i dati è chiuso a chiave; |
| S12 | Predisposizione di misure antincendio (scaffali ignifughi, iniettori ad acqua) |
| S13 | Il locale è chiuso se non presidiato |
| S14 | Misure anti effrazione |
| S15 | Sistemi di teleallarme |
| … | |

## 8) Informativa specifica per i dipendenti (da consegnare al momento dell'assunzione)

FAC-SIMILE INFORMATIVA DIPENDENTI

L'informativa dovrà essere rilasciata all'interessato [30]:
*a) al momento della raccolta dei dati presso l'interessato, nel momento in cui i dati personali sono ottenuti (art.13 Reg (UE) 2016/679);*
*b) se i dati personali non sono raccolti presso l'interessato, entro:*
*- un termine ragionevole dall'ottenimento dei dati, ma al più tardi entro un mese;*
*- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;*
*- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali (art. 14 num. 3 Reg (UE) 2016/679) .*

*Si sottolinea che, qualora nell'ambito del rapporto di lavoro, vengano trattati dati personali relativi ai familiari, non minorenni, dei lavoratori (per esempio: stato di gravidanza della moglie, stato di salute, grave infermità del familiare, stato di handicap del figlio, familiari a carico, ecc…), anche ad essi dovrà essere rilasciata apposita informativa e richiesto il relativo consenso.*

Il testo qui riportato rappresenta semplicemente una bozza per la redazione dell'informativa che dovrà essere fornita ai dipendenti e pertanto dovrà essere adattata alla realtà organizzativa ed operativa della singola impresa.

---

*(Redigere su carta intestata della società)*

Egr. Sig. / Gent.ma Sig.ra

_____

**Oggetto: informativa resa all'interessato per il trattamento[31] dei dati personali comuni e sensibili** [32]

Ai sensi degli artt. 13 e 14 *Reg (UE) 2016/679*, ed in relazione ai dati personali che si intendono trattare, La informiamo di quanto segue:

1. il trattamento a cui saranno sottoposti i dati personali comuni e sensibili richiesti o acquisiti sia preventivamente all'instaurazione del rapporto di lavoro, che nel corso e dopo la cessazione dello stesso nonché acquisiti tramite gli strumenti di cui ai commi 1 e 2 dell'art. 4 legge 300/1970, sarà effettuato al fine dell'instaurazione e gestione del rapporto di lavoro e della gestione previdenziale, nonché per adempiere ad ogni altro obbligo derivante dal contratto individuale, dal contratto collettivo, dalle leggi, regolamenti e normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di formazione, di igiene e sicurezza del lavoro e di previdenza e assistenza, per provvedere, in particolare, agli adempimenti

[30] ex art.4 num 1), Reg (UE) 2016/679, "interessato": la 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

[31] ex art.4 num 2) Reg (UE) 2016/679, "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;

[32] ex art.4 num 1) Reg (UE) 2016/679, "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;

retributivi, contributivi, di assicurazione e fiscali, connessi alla corresponsione delle paghe ed ai relativi adempimenti di legge nonché al fine dell'esercizio del potere disciplinare per contestare eventuali inadempimenti nell'esecuzione del rapporto di lavoro. Il trattamento è compiuto per adempiere ad obblighi contrattuali, nonché di legge cui è soggetto il titolare. [33]

2. il trattamento è effettuato nel rispetto dei principi e delle modalità previste dal *Regolamento 2016/679/UE*, in particolare degli artt. 5 e 6 e 22[34], comprenderà tutte le operazioni o complesso di operazioni previste all'art.4 num. 2), *Regolamento 2016/679/UE*, , necessarie al trattamento in questione, ivi inclusa la comunicazione nei confronti dei soggetti di cui al successivo punto 5), nonché la diffusione nell'ambito richiamato al punto 7) della presente informativa; il trattamento avviene nel modo seguente:……[35];
3. il conferimento dei dati personali relativi al trattamento in parola ha natura ……. (*obbligatoria/facoltativa)*. Base giuridica del trattamento è _____ *(*indicare una delle seguenti ipotesi: *consenso dell'interessato, il dover dare esecuzione ad un contratto, un obbligo legale, l'interesse legittimo del titolare del trattamento)*;
4. l'eventuale, parziale o totale, rifiuto di rispondere comporterà ……. *(indicare le conseguenze)* [36];
5. i dati personali relativi al trattamento in questione, per le finalità di cui al punto 1), verranno comunicati a ……..[37];
6. dei dati forniti potranno venire a conoscenza i seguenti responsabili o incaricati[38] del trattamento ……[39];
7. i dati personali in questione potranno/non potranno essere diffusi *(specificare l'ambito di diffusione, per es. nell'ambito dello Stato italiano)* e trasferiti all'estero ….. (specificare se il Paese terzo indicato ha ricevuto una decisione di adeguatezza dalla Commissione europea[40] o, in caso contrario, se si utilizzano BCR[41] di gruppo ove trasferiti all'interno di gruppi di imprese oppure se sono state inserite specifiche clausole contrattuali modello) *specificare se all'interno della UE o meno e gli Stati di destinazione, nonché l'esistenza*

---

[33] inserire quest'ultimo periodo solo se i dati raccolti sono utilizzati per finalità ulteriori rispetto all'adempimento di obblighi di legge o contrattuali.

[34] citare tale articolo solo se il trattamento è effettuato attraverso processi decisionali automatizzati o che ne comportano la profilazione. In tal caso è necessario fornire informazioni circa la logica utilizzata, nonché L'importanza e le conseguenze previste per l'interessato.

[35] Per esempio:
- il trattamento è effettuato con o senza l'utilizzo di strumenti elettronici e gestito da personale appositamente incaricato;
- la conservazione dei dati avverrà in forma cartacea e/o su supporto magnetico/ informatico/ottico;
- i trattamenti di tipo manuale con raccolta dei dati medesimi su appositi registri e/o schede la cui conservazione sarà attuata con archiviazione tradizionale in appositi contenitori.

[36] Per esempio:l'impossibilità di perseguire in tutto o in parte le finalità indicate al punto 1);

[37] Indicare gli eventuali destinatari o le categorie dei soggetti ai quali possono essere comunicati i dati personali. Si richiamano qui di seguito, a titolo esemplificativo:
- alle pubbliche amministrazioni, con i criteri e nei limiti stabiliti dalla normativa vigente;
- alle organizzazioni sindacali dei lavoratori per gli adempimenti conseguenti all'attuazione delle trattenute sindacali;
- ai fondi o casse di previdenza e assistenza, al fine di …….. (per es.; iscrizione, gestione del conto individuale);
- alla Società ……..: ai fini della riscossione del premio relativo alla polizza ……..;
- alla Società ……..: ai fini della gestione del servizio paghe e contributi;
- al personale di Società esterne addette alla gestione e manutenzione dei sistemi informatici;
- ai rappresentanti dei lavoratori per la sicurezza quando gli stessi esercitino il diritto di accesso previsto dall'art. 50, comma 5, del D.Lgs. 81/2008;
- all'Organismo Paritetico Provinciale, relativamente al nominativo del Rappresentante dei Lavoratori per la Sicurezza;
- alle organizzazioni e/o alle aziende appartenenti al sistema Confindustria (con riguardo al personale dirigente avente eventuali incarichi sindacali in organismi delle associazioni dei datori di lavoro), a scopo informativo e per lo svolgimento dell'incarico;
- ad altre società facenti parte del gruppo, al fine di scambio di servizi e prestazioni tra le Società stesse;
- alle A.P.L. e società di formazione, per attività di formazione e/o supporto agli inserimenti al lavoro;
ecc.

[38] ex art.4 num 8), Reg (UE) 2016/679 «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;

[39] Indicare i soggetti o le categorie di soggetti che possono venire a conoscenza dei dati raccolti, in qualità di responsabili o incaricati. Bisognerà specificare se i dati saranno trattati dai dipendenti dell'impresa (ad es. addetti ufficio amministrazione e personale) o dati in outsourcing (ad es. nomina di una società esterna come responsabile di tutto o parte del trattamento).

[40] E' possibile verificare quali Paesi hanno ricevuto una decisione di adeguatezza consultando http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1;

[41] Bcr è l'acronimo di "binding corporate rules" ovvero regole vincolanti infragruppo che offrano pari garanzia di tutela dei dati rispetto alla normativa comunitaria.

*o meno di una decisione di adeguatezza in caso di trasferimento ex artt. 46, 47 e 49 c.2 Reg (UE) 2016/679, il riferimento alle garanzie appropriate e opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono resi disponibili)*;

8. I dati personali in questione potranno saranno conservati per il tempo strettamente necessario ad assolvere alle finalità di cui al punto 1. Anche, laddove lo richieda la legge, successivamente alla cessazione del rapporto di lavoro e, comunque, non oltre ____ anni dalla cessazione del predetto rapporto.
9. all'interessato dal trattamento in esame è riconosciuto l'esercizio dei diritti di cui agli artt. 15, 16, 17, 18, 20, 21, *Reg (UE) 2016/679,* il cui testo integrale è riportato in allegato, ivi compreso il diritto di proporre reclamo a un'autorità di controllo;
10. titolare[42] del trattamento in parola è la società _____ *In persona del legale rappresentante pro tempore*; Responsabile per la protezione dei dati[43] è il sig. _____ *(precisare gli estremi identificativi del titolare e, laddove nominato del responsabile, nonché del responsabile per la protezione dei dati[44], precisando le modalità per reperire il nominativo aggiornato del responsabile, i dati di contatto del medesimo. Se è stato designato un responsabile per il riscontro all'interessato, è indicato tale responsabile.)*. Amministratore di sistema è il sig _____.

_____ lì _____

Timbro e firma del legale rappresentante

Per ricevuta

_____

Firma del lavoratore

---

[42] ex art.4 num 7), Reg (UE) 2016/679, «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;

[43] Responsabile della porotezione dei dati - art. 37 Reg (UE) 2016/679

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5.Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

[44] È necessario nominare un responsabile per la protezione dei dati ogni qualvolta l'attività principale del titolare del trattamento (o del responsabile) consistano nel trattamento, su larga scala , di categorie particolari di dati personali di cui all'articolo 9 (dati sensibili, es. tessere sindacali) o di dati relativi a condanne penali e reati di cui all'art. 10, nonché qualora il trattamento richieda il monitoraggio regolare e sistematico degli interessati su larga scala.

**Fac- simile di consenso al trattamento dei dati personali del lavoratore (*da aggiungere in calce all'informativa se il trattamento è basato, in tutto o in parte, sul consenso)**

Spett.le

_____

**Oggetto: consenso al trattamento dei miei dati personali**

Io sottoscritto _____, preso atto dell'informativa ex artt. 13 e 14, Reg. 679/2016/UE ed avuta integrale conoscenza delle informazioni in esso contenute, nonché dei diritti a me riconosciuti dagli artt. 15, 16, 17, 18, 20, 21, *Reg. 2016/679/UE,* ivi compreso il diritto di proporre reclamo a un'autorità di controllo, do atto che il trattamento è necessario per l'esecuzione del contratto di lavoro e, per quanto attiene ai seguenti specifici trattamenti:

- con riguardo al trattamento dei miei dati sensibili per le finalità indicate al punto 1 della menzionata informativa:

[ ] do il consenso [ ] nego il consenso

- con riguardo al trasferimento dei miei dati, anche sensibili, verso Paesi esteri o organizzazioni internazionali ex art. 44 e ss:[45]

[ ] do il consenso dichiaro di essere stato informato dei rischi derivanti da siffatto trasferimento, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate

[ ] nego il consenso

- con riguardo all'attività di profilazione dei miei dati o alle decisioni su di essi prese attraverso processi automatizzati, ex art. 22 del Reg. 2016/679/UE[46]

[ ] do il consenso [ ] nego il consenso

[45] da inserire solo nel caso in cui i dati siano trasferiti verso Paesi esteri che non abbiano ricevuto una decisione di adeguatezza, o qualora, nell'ambito di trasferimenti di dati infragruppo, nei rapporti con l'azienda ricevente situata nel Paese estero non siano stipulate delle norme vincolanti d'impresa (BCR). Se il trasferimento avviene in un Paese estero che ha ricevuto una decisione di adeguatezza non è necessario il consenso.

[46] Consenso da inserire solo nel caso in cui vengano effettuate attività di profilazione dei dati del lavoratore dipendente;

***Fac-simile di Informativa ai FAMILIARI del lavoratore dipendente(*) per il trattamento dei loro dati personali***

*Il testo qui riportato rappresenta semplicemente una bozza per la redazione dell'informativa che dovrà essere fornita ai familiari dei dipendenti e pertanto dovrà essere adattata alla realtà organizzativa ed operativa della singola impresa.*

---

*(Redigere su carta intestata della società)*

Oggetto: informativa resa all'interessato per il trattamento[47] dei dati personali comuni e sensibili [48]

Ai sensi degli artt. 13 e 14 *Reg (UE) 2016/679*, ed in relazione ai dati personali che si intendono trattare, La informiamo di quanto segue:

1. il trattamento a cui saranno sottoposti i dati personali comuni e sensibili richiesti o acquisiti sia preventivamente all'instaurazione del rapporto di lavoro con il suo familiare, sarà effettuato al fine della gestione del rapporto di lavoro, nonché per adempiere ad ogni altro obbligo derivante dal contratto individuale, dal contratto collettivo, dalle leggi, regolamenti e normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di previdenza e assistenza, per provvedere, in particolare, agli adempimenti retributivi, contributivi, di assicurazione e fiscali, connessi alla corresponsione delle paghe ed ai relativi adempimenti di legge;
2. il trattamento è effettuato nel rispetto dei principi e delle modalità previste dagli artt. 5 e 6 ed eventualmente 22[49] del *Reg (UE) 2016/679*, comprenderà tutte le operazioni o complesso di operazioni previste all'art.4 num. 2), *Reg (UE) 2016/679*, necessarie al trattamento in questione, ivi inclusa la comunicazione nei confronti dei soggetti di cui al successivo punto 5), nonché la diffusione nell'ambito richiamato al punto 7) della presente informativa; il trattamento avviene nel modo seguente:……[50];
3. il conferimento dei dati personali relativi al trattamento in parola ha natura obbligatoria. Base giuridica del trattamento è il consenso dell'interessato.
4. l'eventuale, parziale o totale, rifiuto di rispondere comporterà ……. *(indicare le conseguenze)* [51];
5. i dati personali relativi al trattamento in questione, per le finalità di cui al punto 1), verranno comunicati a ……..[52];

[47] ex art.4 num 2) Reg (UE) 2016/679, "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;

[48] ex art.4 num 1) Reg (UE) 2016/679, "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;

[49] citare tale articolo solo se il trattamento è effettuato attraverso processi decisionali automatizzati o che ne comportano la profilazione. In tal caso è necessario fornire informazioni circa la logica utilizzata, nonché L'importanza e le conseguenze previste per l'interessato.

[50] Per esempio:
- il trattamento è effettuato con o senza l'utilizzo di strumenti elettronici e gestito da personale appositamente incaricato;
- la conservazione dei dati avverrà in forma cartacea e/o su supporto magnetico/ informatico/ottico;
- i trattamenti di tipo manuale con raccolta dei dati medesimi su appositi registri e/o schede la cui conservazione sarà attuata con archiviazione tradizionale in appositi contenitori.

[51] Per esempio:l'impossibilità di perseguire in tutto o in parte le finalità indicate al punto 1);

[52] Indicare gli eventuali destinatari o le categorie dei soggetti ai quali possono essere comunicati i dati personali. Si richiamano qui di seguito, a titolo esemplificativo:

6. dei dati forniti potranno venire a conoscenza i seguenti responsabili o incaricati[53] del trattamento ……[54];
7. i dati personali in questione potranno/non potranno essere diffusi *(specificare l'ambito di diffusione, per es. nell'ambito dello Stato italiano)* e trasferiti all'estero ….. (specificare se il Paese terzo indicato ha ricevuto una decisione di adeguatezza dalla Commissione europea[55] o, in caso contrario, se si utilizzano BCR[56] di gruppo ove trasferiti all'interno di gruppi di imprese oppure se sono state inserite specifiche clausole contrattuali modello) *specificare se all'interno della UE o meno e gli Stati di destinazione, nonché l'esistenza o meno di una decisione di adeguatezza in caso di trasferimento ex artt. 46, 47 e 49 c.2 Reg (UE) 2016/679, il riferimento alle garanzie appropriate e opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono resi disponibili)*;
8. I dati personali in questione potranno saranno conservati per il tempo strettamente necessario ad assolvere alle finalità di cui al punto 1. Anche, laddove lo richieda la legge, successivamente alla cessazione del rapporto di lavoro e, comunque, non oltre ____ anni dalla cessazione del predetto rapporto in essere con il suo familiare.
9. all'interessato dal trattamento in esame è riconosciuto l'esercizio dei diritti di cui agli artt. 15, 16, 17, 18, 20, 21, *Reg (UE) 2016/679,* il cui testo integrale è riportato in allegato, ivi compreso il diritto di proporre reclamo a un'autorità di controllo;
10. titolare[57] del trattamento in parola è la società _____ *In persona del legale rappresentante pro tempore*, Responsabile per la protezione dei dati[58] è il sig. _____ *(precisare gli estremi*

---

- ai fondi o casse di previdenza e assistenza, al fine di …….. (per es.; iscrizione, gestione del conto individuale);
- alla Società ……..: ai fini della riscossione del premio relativo alla polizza ……..;
- alla Società ……..: ai fini della gestione del servizio paghe e contributi;
- al personale di Società esterne addette alla gestione e manutenzione dei sistemi informatici;
- alle organizzazioni e/o alle aziende appartenenti al sistema Confindustria (con riguardo al personale dirigente avente eventuali incarichi sindacali in organismi delle associazioni dei datori di lavoro), a scopo informativo e per lo svolgimento dell'incarico;
- ad altre società facenti parte del gruppo, al fine di scambio di servizi e prestazioni tra le Società stesse;

[53] ex art.4 num 8), Reg (UE) 2016/679 «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;

[54] Indicare i soggetti o le categorie di soggetti che possono venire a conoscenza dei dati raccolti, in qualità di responsabili o incaricati. Bisognerà specificare se i dati saranno trattati dai dipendenti dell'impresa (ad es. addetti ufficio amministrazione e personale) o dati in outsourcing (ad es. nomina di una società esterna come responsabile di tutto o parte del trattamento).

[55] E' possibile verificare quali Paesi hanno ricevuto una decisione di adeguatezza consultando http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1;

[56] Bcr è l'acronimo di "binding corporate rules" ovvero regole vincolanti infragruppo che offrano pari garanzia di tutela dei dati rispetto alla normativa comunitaria.

[57] ex art.4 num 7), Reg (UE) 2016/679, «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;

[58] Responsabile della porotezione dei dati - art. 37 Reg (UE) 2016/679

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5.Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

*identificativi del titolare e, laddove nominato del responsabile, nonché del responsabile per la protezione dei dati*[59]*, precisando le modalità per reperire il nominativo aggiornato del responsabile, i dati di contatto del medesimo. Se è stato designato un responsabile per il riscontro all'interessato, è indicato tale responsabile.)*.

……. lì ……..

Timbro e firma del legale rappresentante

Per ricevuta

_____

Firma del lavoratore

All.: Art. 15, 16, 17, 18, 20, 21 *Reg (UE) 2016/679*

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

[59] È necessario nominare un responsabile per la protezione dei dati ogni qualvolta l'attività principale del titolare del trattamento (o del responsabile) consistano nel trattamento, su larga scala , di categorie particolari di dati personali di cui all'articolo 9 (dati sensibili, es. tessere sindacali) o di dati relativi a condanne penali e reati di cui all'art. 10, nonché qualora il trattamento richieda il monitoraggio regolare e sistematico degli interessati su larga scala.

***Fac-simile di consenso al trattamento dei dati personali dei familiari del lavoratore****(*)*

*(*) Modello da aggiungere in calce all'informativa se sono fornite informazioni e/o dati relativi ai familiari del lavoratore dipendente (per esempio per richieste di detrazioni fiscali, assegno per il nucleo familiare, ecc..)*

I sottoscritti, come sotto identificati, familiari del Sig. ……. , dipendente della Società ……. dichiarano di aver ricevuto dalla medesima Società completa informativa ai sensi degli artt. 13 e 14 *Reg (UE) 2016/679*, unitamente a copia degli artt. 15, 16, 17, 18, 20, 21 del medesimo Regolamento ed esprimono il loro consenso al trattamento ed alla comunicazione dei propri dati personali conferiti alla predetta Società, con particolare riguardo a quelli definiti "sensibili" o comunque definiti come "genetici", "biometrici" o "relativi alla salute" ex art. 4 del Regolamento, nei limiti, per le finalità precisate al punto 1 dell'informativa.

| Nome e cognome del familiare | Grado di parentela | Data | Firma |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

*NOTA BENE*

*Il modulo di consenso deve essere compilato con i dati dei familiari. La capacità d'agire in ambito privacy si acquisisce al compimento del sedicesimo anno di età. Pertanto, dovrà essere lo stesso familiare sedicenne o diciassettenne a dover firmare il consenso al trattamento dei suoi dati personali.*

## 9) Check list privacy

*La presente check list è esemplificativa e non esaustiva dei principali adempimenti privacy.*

**1) INFORMATIVA E CONSENSO**

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| Ho predisposto le seguenti informative: | | |
| - dipendenti; | | |
| - clienti persone fisiche; | | |
| - candidature non spontanee (CV) | | |
| Sito internet: | | |
| a)informativa sito; | | |
| b)policy utilizzo cookie; | | |
| c) informativa invio CV; | | |
| d) informativa invio newsletter; | | |
| - informativa videosorveglianza; | | |
| - informativa geolocalizzazione[60]; | | |
| - informativa biometrico[61]; | | |
| Marketing diretto: | | |
| - informativa invio comunicazioni commerciali; | | |
| - ho richiesto il consenso agli interessati;[62] | | |
| Profilazione e processi decisionali automatizzati: | | |
| - informativa; | | |
| - consenso[63] | | |

**2) NOMINE/FIGURE PRIVACY**

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - contitolare del trattamento[64]; | | |
| - persone autorizzate e/o incaricati del trattamento[65]; | | |
| - amministratore di sistema[66]; | | |
| - custode delle credenziali[67]; | | |

[60] Es. veicoli geolocalizzati, telefonini geolocalizzati ecc…

[61] Es. in caso di timbratura delle presenze mediante impronta digitale, oppure in caso di accesso in area aziendali attraverso l'impronta.

[62] Il consenso deve essere prestato secondo i criteri e le modalità stabilite dagli artt. 6 e 7. Il consenso è richiesto quando si trattano dati di minori, oppure quando sto facendo attività di "marketing profilato".

[63] È sempre richiesto il consenso per attività di profilazione e quando i processi decisionali automatizzati sui dati dell'interessato siano l'unico fondamento di una decisione del Titolare del trattamento;

[64] È necessario nominare un contitolare del trattamento qualora un trattamento sia effettuato da più soggetti (es. videosorveglianza di locali comuni). Si ricorda, che le responsabilità in merito all'osservanza degli obblighi previsti dal GDPR è ripartita dai contitolari attraverso un accordo interno che evidenzi i rispettivi ruoli nell'ambito del trattamento.
L'accordo deve prevedere dunque una ripartizione degli obblighi del Regolamento (es. esercizio dei diritti dell'interessato), le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del Regolamento. L'accordo, inoltre, deve essere messo a disposizione dell'interessato.

[65] pur non essendo espressamente prevista una nomina per le persone autorizzate al trattamento potrebbe essere comunque opportuno fornire loro istruzioni scritte attraverso un atto unilaterale di nomina;

[66] La nomina con la descrizione dell'ambito di operatività e delle funzioni dell'ADS deve essere conservata e aggiornata in caso di accertamenti anche da parte del Garante.

| | | |
|---|---|---|
| - responsabile per la protezione dei dati (RPD/DPO)[68]; | | |
| Responsabili esterni del trattamento (se presenti): | | |
| - medico competente; | | |
| - studio paghe; | | |
| - manutenzione | | |
| Ecc… | | |

3) Principi[69]:

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - i dati sono trattati in modo lecito e secondo correttezza; | | |
| - i dati sono raccolti per scopi determinati, espliciti e legittimi; | | |
| - i dati sono esatti e aggiornati | | |
| - i dati sono pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti; | | |
| - i dati sono conservati solo per il tempo strettamente necessario ad assolvere la finalità per cui sono trattati; | | |

4) Misure di sicurezza

a) Trattamenti elettronici - Compiti amministratore di sistema[70]

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - Credenziali di autenticazione informatica per chi tratta i dati (incaricati)[71]; | | |
| - modifica credenziale ogni 6 mesi (trattamento solo di dati comuni) oppure ogni 3 mesi (anche dati sensibili e giudiziari) | | |
| - disattivazione credenziali non utilizzate | | |

[67] è possibile far combaciare questa figura con quella dell'amministratore di sistema, purché sia espressamente previsto nella lettera di nomina.

[68] In base all'articolo 37, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:
a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.
Per ulteriori approfondimenti in argomento v. Linee guida sul data protection officer del WP29 del 16.12.2016.

[69] E' necessario rispettare, durante il trattamento dei dati i principi per il trattamento dei dati dall'art. 5 del Regolamento 679/2016/UE non differiscono da quelli del d.lgs. 196/03.

[70] Anche dopo l'entrata in vigore del Regolamento Europeo 679/2016/UE, e la conseguente abrogazione del Codice della privacy, è necessario che l'ADS continui a predisporre le misure minime previste nell'Allegato B del Codice della Privacy, poiché indirettamente richiamate dal provv. Generale del 27 novembre 2008.

[71] La credenziale deve essere di almeno 8 caratteri e non deve contenere riferimenti direttamente riconducibili all'incaricato;

| | | |
|---|---|---|
| da almeno 6 mesi (salvo che servano per la gestione tecnica)[72]; | | |
| - istruzioni agli incaricati (policy) in cui si dice di non lasciare incustodito e accessibile lo strumento (es. pc) | | |
| - aggiornamento almeno semestrale dei sistemi di protezione (antivirus, firewall ecc…) | | |
| - sistemi di backup and restore dei dati (entro 7 giorni in caso di dati sensibili e giudiziali); | | |
| - sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili in cui sono memorizzati dati sensibili e giudiziali; | | |
| - distruzione dei predetti supporti in caso di mancato utilizzo; | | |
| - ai dipendenti è fornita l'identità degli ADS mediante apposita informativa ex art. 13 del Codice se la loro attività riguardi anche indirettamente servizi e sistemi che trattino o permettano il trattamento di informazioni di carattere personale di lavoratori[73]; | | |
| - è stato verificato l'operato dell'amministratore di sistema almeno con cadenza annuale; | | |
| - gli accessi dell'amministratore di sistema sono registrati tramite file di log conservati per almeno 6 mesi e presentano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. | | |

b) trattamenti senza l'ausilio di strumenti elettronici

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - sono fornite istruzioni scritte agli incaricati finalizzate al controllo e alla custodia relativamente al trattamento dei dati[74]; | | |
| - i dati di natura giudiziale e sensibile affidati ai responsabili o agli incaricati sono custoditi fino alla restituzione senza che ne sia consentito l'accesso ad altre persone; | | |
| - i dati archiviati sono tenuti al sicuro attraverso misure di sicurezza idonee | | |

[72] La credenziale deve essere disattivata anche qualora perda la qualità che consente all'incaricato l'accesso ai dati personali;
[73] è possibile inserire la predetta informativa nella lettera di
[74] tale obbligo può essere assolto indicando nella lettera di nomina le istruzioni (già presenti nei modelli associativi);

| | | |
|---|---|---|
| (armadi ignifughi ecc…) | | |

c) Misure tecniche e organizzative (adeguate). Le misure di sicurezza sono state predisposte tenendo in considerazione i seguenti fattori:

| **Principio** | ✓ | **Osservazioni/Note** |
|---|---|---|
| Stato dell'arte e costi di attuazione | | |
| Natura del trattamento | | |
| Oggetto del trattamento | | |
| Contesto aziendale | | |
| Finalità del trattamento | | |
| Probabilità e rischi per i diritti e libertà delle persone fisiche | | |

Nel rispetto dei suddetti principi sono state predisposte misure di sicurezza che comprendono:

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - Pseudonomizzazione e cifratura dei dati personali; | | |
| - capacità di garantire in maniera permanente la riservatezza, integrità, disponibilità e resilienza[75] dei sistemi e dei servizi di trattamento; | | |
| - capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; | | |
| - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative implementate | | |

d) registro dei trattamenti

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - Ho predisposto un registro dei trattamenti[76] | | |

e) valutazione d'impatto privacy

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - Ho predisposto una VIP per tutti quei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati al trattamento | | |

[75] La **resilienza** è la capacità di un sistema di adattarsi al cambiamento, di saper resistere a pressioni esterne (tentativi di intrusione nei sistemi, di cancellazione fraudolenta dei dati ecc…)
[76] V. modulo 7 della guida;

**6) TRATTAMENTI SPECIFICI**

a) Videosorveglianza

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - informativa minima (cartello) | | |
| - informativa completa; | | |
| - accordo sindacale/autorizzazione della DTL; | | |
| - nomina incaricati visualizzazione immagini in tempo reale; | | |
| - nomina incaricati visualizzazione immagini registrate; | | |
| - nomina responsabile/incaricato servizio di manutenzione del sistema[77]; | | |
| - informativa art. 4 co. 3 st.lav. | | |
| - conservazione massimo 24 h con estensione ai periodi di chiusura locali | | |

b) geolocalizzazione (telefonini, gps satellitare macchina ecc…)

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - informativa minima (vetrofania) | | |
| - informativa completa; | | |
| - accordo sindacale/autorizzazione della DTL; | | |
| - nomina incaricati gestione del sistema e dei dati di localizzazione; | | |
| - nomina responsabile/incaricato servizio di manutenzione del sistema[78]; | | |
| - informativa art. 4 co. 3 st.lav. | | |
| - conservazione dati per il periodo strettamente necessario ad assolvere alla finalità per cui il sistema gps è installato; | | |

c) Sito internet

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - informativa e consenso cookie[79]; | | |
| - informativa estesa privacy; | | |
| - informativa e acquisizione consenso invio newsletter; | | |
| - informativa e consenso invio CV; | | |

[77] È necessario effettuare questa nomina qualora il gestore del sistema abbia, anche solo potenzialmente, la possibilità di trattare il dato;
[78] È necessario effettuare questa nomina qualora il gestore del sistema abbia, anche solo potenzialmente, la possibilità di trattare il dato;
[79] v. Provv. 8 maggio 2014 (modalità per rendere informativa semplificata cookie)

d) biometria

| **Adempimento** | ✓ | **Osservazioni/Note** |
|---|---|---|
| - informativa; | | |
| - accordo sindacale/autorizzazione della DTL[80]; | | |
| - nomina incaricati al trattamento dei dati biometrici; | | |
| - nomina responsabile/incaricato servizio di manutenzione del sistema di rilevazione biometrica[81]; | | |
| - informativa art. 4 co. 3 st.lav.[82] | | |
| - notifica preliminare al Garante | | |
| - conservazione dati per il periodo strettamente necessario ad assolvere alla finalità; | | |

[80] Solo laddove dall'installazione possa derivare un controllo a distanza;
[81] È necessario effettuare questa nomina qualora il gestore del sistema abbia, anche solo potenzialmente, la possibilità di trattare il dato;
[82] Solo laddove dall'installazione possa derivare un controllo a distanza;