ANCE | ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

Direzione Relazioni Industriali

Guida per le imprese

PRIVACY

GDPR - General Data Protection Regulation

REGOLAMENTO UE N. 2016/679

MARZO 2018

a cura di Bianca Maria Baron e Valeria Andretta, Relazioni Industriali ANCE

Guida per le imprese

PRIVACY

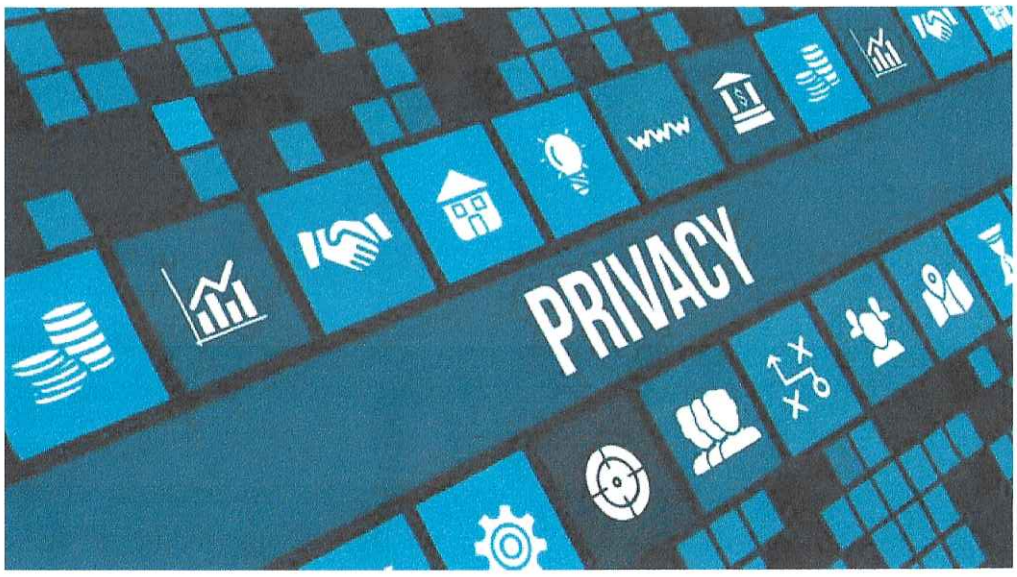
GDPR - General Data Protection Regulation
REGOLAMENTO UE N. 2016/679

MARZO 2018

a cura di Bianca Maria Baron e Valeria Andretta, Relazioni Industriali ANCE

EDILSTAMPA srl
via G.A. Guattani 20 - 00161 Roma
tel. 0684567403 - fax 0684567590
edilstampa@ance.it - www.edilstampa.it

SOMMARIO



1. INTRODUZIONE

Applicabilità del GDPR

Il **25 maggio 2018** diventerà applicabile, in tutti gli Stati membri, il Nuovo Regolamento Europeo (**GDPR - *General Data Protection Regulation***) *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, (in vigore dal 24 maggio 2016).

Il Nuovo Regolamento promuove la tutela dei dati personali basata sulla responsabilizzazione dei titolari del trattamento dati (c.d. accountability).

La logica propria del Regolamento è, infatti, quella di procedere ad una messa a punto di processi interni delle imprese (o degli Enti o di tutti coloro che trattano dati personali) che, partendo da una valutazione dei rischi sull'utilizzo dei dati stessi, possa mettere in atto sistemi di tutela *ad hoc*.

Alcuni dei principi della precedente normativa rimarranno validi anche con l'attuazione del nuovo Regolamento (l'obbligo di informativa, il consenso dell'interessato, la distinzione tra dati personali e dati sensibili). Altri, invece, rappresentano delle novità o parzialmente tali (la denominazione degli attori – il titolare del trattamento, il responsabile del trattamento, i corresponsabili, il responsabile della protezione dati, il diritto all'oblio, il data breach, l'accountability).

Per alcune realtà sarà necessario dotarsi anche di un Responsabile della protezione dei dati (RPD)/Data Protection Officer (DPO), ossia di una figura specializzata che assicuri la corretta gestione delle informazioni.

Scompariranno alcuni oneri amministrativi, quali ad esempio quelli di notificazione anticipata di particolari trattamenti al Garante; in tal senso, si parla di ***una maggiore responsabilizzazione a fronte di una semplificazione***.

Si passa da un sistema prescrittivo per i titolari ad un sistema che, attuando un cambio di mentalità, vuole che il titolare parta da una valutazione di ogni singola realtà ove si attua un trattamento dei dati per capire quali sono i rischi di ogni singolo trattamento e attuare i sistemi di sicurezza adeguati alla tutela di tali dati, garantendone la **confidenzialità**, l'**integrità** e la **disponibilità**.

Nelle realtà imprenditoriali, pertanto, il titolare dovrà effettuare le valutazioni del caso per ridurre al minimo il trattamento dei dati dei propri dipendenti e, in particolare, per utilizzare i dati necessari di ciascun dipendente unicamente per le specifiche finalità previste dal trattamento oggetto di informativa e consenso.

Stante la carenza di precisi riferimenti per molti degli istituti descritti nel Regolamento e l'indeterminatezza di alcune regole e della loro attuazione, le disposizione regolamentari dovranno essere oggetto di specifici interventi da parte delle c.d. Autorità di controllo dei singoli Stati membri (in Italia l'Autorità Garante), o singolarmente o attraverso iniziative congiunte, al livello europeo, da recepire poi nei singoli Stati membri (ad esempio linee guida ad hoc).

La guida intende fornire un primo supporto per le imprese che approcciano con il nuovo Regolamento e che troveranno sempre gli uffici Ance a loro disposizione per i chiarimenti del caso.

2. I PRINCIPI GENERALI (ARTT. 24-25)

Nuovo quadro giuridico

Il legislatore comunitario ha adottato un Regolamento per rendere più omogenea l'applicazione delle norme sulla Privacy su tutto il territorio comunitario.
Il Regolamento, infatti, è direttamente applicabile in tutti gli Stati membri.
La conformità (***compliance***) al Regolamento deve essere interpretata quale necessità per le imprese per la corretta tutela dei dati trattati.

La responsabilizzazione Accountability

Il Nuovo Regolamento è incentrato sul concetto di responsabilizzazione (***cd accountability***) del titolare, nel senso di attuare tutte le misure necessarie per una corretta *compliance* al Regolamento.
Rientra nel concetto di responsabilizzazione del titolare, a titolo esemplificativo, il compito di effettuare, anche tramite il DPO (ove nominato) o attraverso un responsabile interno, la valutazione dei rischi del trattamento dei dati, l'attuazione delle misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, la redazione del registro dei dati.

Privacy by design - Privacy by default

Per tale ragione si parla di Privacy by design, nel senso di definire il trattamento dati in ottemperanza al Regolamento dimostrando di aver fatto tutto il possibile per evitare il rischio, e di Privacy by default, nel senso di aver adottato tutti gli strumenti tecnologici per proteggere il dato.

3. IL TRATTAMENTO DEI DATI (ART. 4.2)

Tipologie di trattamento

Il trattamento dei dati consiste in qualsiasi operazione compiuta anche senza l'ausilio dei processi automatizzati, concernente la raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, estrazione, consultazione, uso, comunicazione, messa a disposizione, raffronto, interconnessione, limitazione, cancellazione, diffusione, distruzione dei dati.

I principi generali del trattamento

Il trattamento dei dati deve essere orientato al rispetto dei seguenti principi:

- liceità, correttezza e trasparenza;
- minimizzazione/pertinenza/proporzionalità (trattamento adeguato e proporzionato alle finalità che devono essere determinate, esplicite e legittime);
- limitazione alla conservazione;
- sicurezza e integrità (mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e della perdita, dalla distrazione o dal danno accidentali).

4. I DATI (ART. 4 E ART. 9)

Dati personali

Si tratta di qualsiasi informazione riguardante una persona fisica identificata o identificabile (nome, dati anagrafici, dati relativi all'ubicazione, codice fiscale, carta di credito, identificativo on line, stato di salute, immagine, voce etc...).

Si dividono in:

dati anagrafici/identificativi

- nome e cognome
- indirizzo di casa
- indirizzo email
- numero di passaporto
- indirizzo IP (quando collegato ad altri dati)
- numero di targa del veicolo
- numero di patente
- numeri di carta di credito
- data di nascita
- numero di telefono
- nickname

dati particolari

- ex dati sensibili (origine razziale, opinione politica, convinzione religiosa, appartenenza sindacale, orientamento sessuale, stato di salute etc...);
- dati genetici
- dati biometrici

altri dati

- dati penali (condanne penali, reati, connessi a misure di sicurezza)
- dati che presentano rischi per la libertà/dignità della persona e sono soggetti alla Valutazione d'impatto DPIA (es. trattamenti su larga scala, geolocalizzazione, videosorveglianza)
- dati comuni (anagrafici, indirizzi postali, indirizzi IP, conto corrente etc...)
- dati anonimi (sui quali non si applica il Regolamento)

5. I SOGGETTI (ART. 4)

Titolare

La persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (impresa).

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

- responsabile interno impresa;
- qualsiasi outsourcers a cui sono trasferiti i dati (es. società esterna incaricata per l'elaborazione delle buste paga).

Incaricati

Tutti coloro che hanno accesso ai dati (es. impiegati ufficio del personale).

Responsabile protezione dati (DPO) (Art. 37)

Il DPO (Data Protection Officer) è colui che, in una posizione di indipendenza dal titolare e dal responsabile, sorveglia il rispetto del Regolamento, della cui inosservanza rimangono unici responsabili il titolare e il responsabile del trattamento.

Non sempre è obbligatoria la nomina del DPO, che riguarda solo i casi di trattamento di dati che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala o comunque il caso di trattamenti su larga scala di dati particolari (ex dati sensibili).

Sembrerebbe quindi che per le imprese edili del comparto tale obbligo non sussista.

Ciò non toglie che un'impresa possa determinarsi comunque di nominare un DPO mediante un contratto di designazione nel quale vengono indicate tutte le funzioni ad esso attribuite. Potrebbe essere nominato unico DPO anche in un gruppo di imprese.

La nomina del DPO deve essere comunicata all'Autorità di controllo (Garante).

Il DPO deve possedere un'idonea professionalità data dalla conoscenza della normativa (GDPR), del settore di attività e della specifica struttura dell'impresa (formazione adeguata e continua).

Il DPO svolge:

- attività di sorveglianza del corretto adempimento del GDPR;
- valutazione dei rischi di ogni trattamento effettuato;
- assistenza al titolare e al responsabile anche nella redazione del Registro dei dati;
- collaborazione per l'eventuale conduzione di una valutazione di impatto (DPIA) laddove si profilino rischi gravi (si ritiene che non è il caso delle imprese edili);
- dialogo con gli interessati con il garante e con tutti coloro che hanno a che fare con il trattamento dati.

Interessati

Coloro i cui dati vengono trattati dal titolare e dai responsabili.

6. I DIRITTI DEGLI INTERESSATI (ARTT. 13-21)

Diritto di informazione	Diritto di ricevere tutte le informazioni relative al trattamento in forma concisa, trasparente, intellegibile e facilmente accessibile (informativa).
Diritto di accesso	Diritto di accedere ai propri dati e ai relativi trattamenti.
Diritto di rettifica	Diritto di rettificare i propri dati con relativo obbligo del titolare di comunicare tali modifiche.
Diritto alla cancellazione (c.d. all'oblio)	Diritto di richiedere la cancellazione dei propri dati quando è esaurita la finalità del trattamento, è stato revocato il consenso, è stata fatta opposizione al trattamento, i dati sono stati trattati in violazione di legge.
Diritto di limitazione	Diritto di limitare il trattamento dei propri dati in caso di inesattezze, di contestazione o come misura alternativa alla cancellazione.
Diritto alla portabilità dei dati	Diritto di trasferire i dati da un titolare a un altro.
Diritto di opposizione	Diritto di opporsi in qualsiasi momento al trattamento dei propri dati personali.

7. I FONDAMENTI DI LICEITÀ DEL TRATTAMENTO (ART. 6)

Il trattamento dei dati è lecito solo in presenza di una delle 6 condizioni previste dal Regolamento:

- esecuzione di un contratto;
- adempimenti ad obblighi di legge;
- salvaguardia degli interessi vitali dell'interessato;
- esecuzione di un compito di interesse pubblico;
- perseguimento di un legittimo interesse del titolare (salvo che non prevalgano i diritti fondamentali dell'interessato);

oppure

- consenso dell'interessato.

Senza il consenso o un'altra condizione di liceità, il trattamento è illecito/sanzionabile.

8. IL CONSENSO (ART. 7)

Il consenso è condizione necessaria per poter trattare i dati in modo lecito, in assenza delle altre condizioni di liceità previste dal Regolamento.
La finalità del consenso è di autorizzare o negare il trattamento dei propri dati personali.

Condizioni del consenso

Il consenso è valido se è:

- informato (preceduto dall'informativa);
- specifico (richiesto in modo chiaro, comprensibile e distinguibile dal resto);
- libero (svincolato da costrizioni);
- consapevole (basato su un'azione positiva inequivocabile).

Pluralità dei consensi

Il consenso, da richiedere in forma scritta (se orale va comunque dimostrato), può essere espresso per una o più finalità diverse, purché sia distinto e separato per ciascuna finalità di trattamento.

Diritto di revoca

L'interessato ha diritto di revocare in qualunque momento il proprio consenso e il titolare ha l'onere di informare l'interessato della possibilità di esercitare tale diritto.

9. L'INFORMATIVA (ART. 13)

È la dichiarazione del titolare ispirata al principio di trasparenza (chiara, intellegibile e concisa) per mettere l'interessato nelle condizioni di conoscere le intenzioni del titolare, le modalità del trattamento e per valutare se accettare o rifiutare il trattamento dei propri dati.

È sempre necessaria anche qualora non sia richiesto il consenso e può essere redatta in qualunque forma (anche orale) purché comprovabile *(accountability)*.
Tempi di consegna:

- al momento della raccolta dei dati;
- entro un mese, se raccolti presso terzi.

10. IL REGISTRO DEI TRATTAMENTI (ART. 30)

Il registro dei trattamenti è un "quadro di censimento e di sintesi", che devono predisporre, in forma scritta, il titolare e il responsabile del trattamento, e contiene le seguenti informazioni:

- nome del titolare (o del responsabile del trattamento o del titolare per cui si agisce);
- descrizione delle attività effettuate dal titolare (o per conto del titolare);
- finalità del trattamento;
- base giuridica del trattamento;
- categorie di dati;
- destinatari dei dati;
- misure di sicurezza adottate;
- termini per la cancellazione dei dati;
- destinatati UE e Extra UE

È obbligatorio per le imprese con più di 250 dipendenti o in tutti quei casi in cui il trattamento non sia occasionale e includa dati particolari (stato di salute, trattenute sindacali, etc...) o che potrebbero provocare rischi per i diritti e le libertà degli interessati.
Si reputa, pertanto, sempre consigliata la sua redazione (accountability).

11. VALUTAZIONE DEL RISCHIO (ART. 32) E VALUTAZIONE D'IMPATTO (DPIA) (ARTT. 35-36)

Ogni qual volta il trattamento dei dati presenta rischi elevati per la libertà e i diritti delle persone fisiche il titolare deve effettuare, prima di procedere al trattamento, la valutazione sul rischio dell'eventuale impatto negativo che il trattamento dei dati può avere sulla libertà e sul diritto degli interessati.
All'esito della valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio.
Anche laddove non si ravvisino rischi elevati sussiste comunque l'obbligo generale del titolare di mettere in atto tutte le misure per gestire in modo idoneo i rischi esistenti, valutati dopo una ordinaria valutazione del rischio (art. 32 nonché ex DPS), che comunque è sempre consigliabile effettuare.

12. IL DATA BREACH - VIOLAZIONE DEI DATI (ARTT. 33-34)

Notifica al garante

Quando un evento comporta la violazione di dati personali (perdita, distruzione o diffusione indebita), il *titolare del trattamento* deve, **entro 72 ore** dal momento in cui ne è venuto a conoscenza (a seguito dell'informazione da parte del responsabile del trattamento), notificare al Garante l'eventuale violazione, comunicando:

- il tipo di violazione;
- il numero degli interessati;
- i dati e i contatti dell'eventuale DPO;
- le possibili conseguenze;
- le misure di contrasto adottate.

L'Autorità di controllo collaborerà con il titolare per mettere in atto tutte le misure necessarie per contenere il danno.

Comunicazione all'interessato

Se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (es. frode, furto d'identità, danno all'immagine, etc...), il titolare del trattamento comunica la violazione anche all'interessato.

13. LA CERTIFICAZIONE (ART. 42)

Caratteristiche

Vi è la possibilità di richiedere l'ausilio di meccanismi di certificazione, sigilli e marchi di protezione dei dati per consentire ai titolari e ai responsabili del trattamento di dimostrare la conformità al Regolamento.

La certificazione è volontaria, accessibile tramite procedura trasparente e non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento.

Può essere rilasciata dal Garante o da altri Enti certificatori accreditati (**non ancora individuati**) ed ha una validità di 3 anni. È rinnovabile e revocabile per perdita dei requisiti.

14. IL REGIME SANZIONATORIO (ARTT. 82-84)

Responsabilità

Il titolare è responsabile per il danno causato dal suo trattamento, mentre il responsabile del trattamento risponde solo se non ha adempiuto agli obblighi previsti dal Regolamento o ha agito in modo difforme rispetto a quanto indicato dal titolare (nel contratto).

Risarcimento del danno

Il titolare o il responsabile del trattamento sono tenuti al risarcimento del danno nei confronti di chiunque subisce un danno materiale o immateriale derivante dalla violazione del trattamento dei dati personali.

Sanzioni amministrative pecuniarie

Sono previste sanzioni amministrative e pecuniarie da € 10.000.000, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di specifiche violazioni a € 20.000.000, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Altre sanzioni

Gli Stati membri possono prevedere l'introduzione di ulteriori sanzioni per le violazioni del Regolamento, che dovranno essere effettive, proporzionate e dissuasive.

15. LA VIDEOSORVEGLIANZA E GLI ALTRI STRUMENTI DI CONTROLLO

Legge n. 300/1970 Art. 4 e s.m.i.

Il controllo da parte del datore di lavoro nei confronti dei lavoratori, tramite impianti audiovisivi e altri strumenti di controllo a distanza, può essere consentito solo per:

- esigenze organizzative e produttive;
- per la sicurezza del lavoro;
- per la tutela del patrimonio aziendale.

Tali impianti possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria (RSU) o dalle rappresentanze sindacali aziendali (RSA) o nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

In mancanza di accordo, gli impianti possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro.

L'accordo **NON** è richiesto:

- per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa;
- per gli strumenti di registrazione degli accessi e delle presenze.

INL Nota n. 299/2017

Per l'***installazione di dispositivi collegati ad impianti di antifurto*** (videocamere o fotocamere) che entrano in funzione *solo* in assenza dei lavoratori, senza possibilità di controllo "preterintenzionale" sul personale, l'istallazione può essere autorizzata in tempi rapidi, stante l'assenza di valutazioni istruttorie.

Solo in tale ipotesi, non sarà, pertanto, necessaria la preventiva procedura di accordo con la RSA o RSU o l'autorizzazione da parte dell'Ispettorato nazionale.

INL Circolare n. 5/2018

Per l'installazione degli impianti di videosorveglianza o di controllo, dovranno emergere in modo chiaro, in ogni richiesta di autorizzazione, le *ragioni organizzative e produttive*, nonché di quelle legate alla *sicurezza del lavoro* e alla *tutela del patrimonio aziendale*.
In particolare, in merito all'**utilizzo di telecamere**, è stato chiarito che:

- l'eventuale ripresa dei lavoratori deve avvenire in via accidentale e occasionale;
- in presenza di ragioni giustificatrici di controllo, è possibile inquadrare direttamente l'operatore senza necessità di oscurarne il volto;
- non è necessario specificare il posizionamento predeterminato e l'esatto numero delle telecamere da installare (fermo restando la coerenza con le ragioni legittimanti il controllo inserite nell'istanza).

Per l'utilizzo di ***sistemi di videosorveglianza*** che si basano ***su tecnologie digitali*** volte all'elaborazione su PC e alla trasmissione su rete dei dati (es. rete IP, cablata o wireless) e che consentono il passaggio di video e audio da un computer all'altro, è stato chiarito che, ove sussistano ragioni giustificatrici del provvedimento, è autorizzabile la visione da postazione remota delle immagini sia in tempo reale che registrate.
La visione in tempo reale delle immagini deve essere autorizzata solo in casi eccezionali.
L'accesso, invece, alle immagini registrate deve essere tracciato, tramite sistemi che consentano la conservazione dei "log di accesso", per un periodo non inferiore a 6 mesi.
Con riferimento all'utilizzo di dispositivi e tecnologie per la raccolta e il ***trattamento dei dati biometrici*** (impronta digitale, topografia della mano) è stato chiarito che, essendo tali sistemi utilizzati per assicurare elevati livelli di sicurezza o per consentire l'utilizzo di macchinari pericolosi, si può considerare l'utilizzo di tali sistemi come "funzionale a rendere la prestazione lavorativa" e, pertanto, non necessitano di accordo sindacale né di procedimento autorizzativo.

16. GLI ADEMPIMENTI PER LE IMPRESE

Nomina dei soggetti privacy

(cfr. punto 5)

IL TITOLARE DEL TRATTAMENTO DATI È L'IMPRESA (LEGALE RAPPRESENTANTE)

IL TITOLARE DEVE NOMINARE UN RESPONSABILE DEL TRATTAMENTO ESTERNO

- **in caso di outsourcing** (es. servizi esterni di buste paga) il responsabile esterno coincide con l'outsourcer e la nomina deve risultare dal contratto di servizi che ne individua i ruoli e le responsabilità
- il responsabile svolge la valutazione del rischio sui dati connessi al contratto di servizi
- il responsabile garantisce l'adozione di misure tecniche organizzative per garantire la sicurezza dei dati oggetto del contratto
- il responsabile si occupa della tenuta del Registro dei trattamenti dei dati oggetto del contratto
- il responsabile assiste il titolare nel rispetto degli obblighi del GDPR

IL TITOLARE PUÒ NOMINARE UN RESPONSABILE DEL TRATTAMENTO INTERNO

- la nomina avviene con lettera di incarico che individua i ruoli e le responsabilità
- il responsabile interno è un dipendente dell'impresa
- svolge la valutazione del rischio
- garantisce l'adozione di misure tecniche organizzatevi per garantire la sicurezza dei dati
- si occupa della tenuta del Registro dei trattamenti
- assiste il titolare nel rispetto degli obblighi del GDPR

IL TITOLARE PUÒ NOMINARE UN RESPONSABILE PER LA PROTEZIONE DEI DATI (DPO)

- la nomina avviene con atto di designazione che individua i ruoli e le responsabilità del DPO
- della nomina va data comunicazione all'Autorità di controllo (Garante)

Redazione documenti

IL TITOLARE E IL RESPONSABILE DEL TRATTAMENTO EFFETTUANO:

1) la Valutazione del rischio (cfr. punto 11)

- **obbligatoria**
- in base alla valutazione vanno individuate le misure di sicurezza da adottare per evitare i rischi (ex DPS)

2) la Valutazione di impatto (DPIA) (cfr. punto 11)

- **non obbligatoria (salvo che il trattamento dei dati implichi un rischio grave per le persone e i diritti)**
- solo quando vi sono rischi connessi alla libertà e i diritti delle persone

3) il Registro dei trattamenti (cfr. punto 10)

- **eventuale (requisiti dimensionali e tipologia dati trattati) ma comunque consigliato**

4) Regolamento/policy interna

- **non obbligatorio ma comunque consigliato**

Tutti i documenti dovranno essere oggetto di monitoraggio e aggiornamento continuo, tenuto conto delle variazioni delle finalità dei trattamenti, dei soggetti, della tipologia dei dati, degli interessati e dei destinatari.

Altri adempimenti

IL TITOLARE DEVE:

1) redigere l'informativa (cfr. punto 9)

- **obbligatoria**
- da presentare agli interessati prima del trattamento dei dati

richiedere il consenso (cfr. punto 8)

- **ove previsto**
- il consenso deve essere richiesto agli interessati dopo aver fornito l'informativa e per ciascun tipo di trattamento.

REGISTRO DELLE ATTIVITÀ DEL TRATTAMENTO DEI DATI PERSONALI[1]

ai sensi dell'art. 30 del Nuovo regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Data ultimo aggiornamento: .....

[1] Le indicazioni contenute nel presente documento hanno carattere esemplificativo e sono state elaborate sulla base delle indicazioni finora fornite dal GDPR e dal Garante e sulla base di quanto emerso in occasione del Gruppo di lavoro presso la Confindustria.
Potranno, pertanto, essere suscettibili di modifiche e/o integrazioni a seguito degli eventuali aggiornamenti.

I SOGGETTI

Titolare del trattamento	
Denominazione o ragione sociale	
Indirizzo	
Telefono	
Indirizzo email	

Contitolare del trattamento	
Denominazione o ragione sociale	
Indirizzo	
Telefono	
Indirizzo email	
Riferimento accordo interno	

Rappresentante del titolare del trattamento (quando il titolare non è stabilito nell'UE)	
Denominazione o ragione sociale	
Indirizzo	
Telefono	
Indirizzo email	
Riferimento atto di designazione	

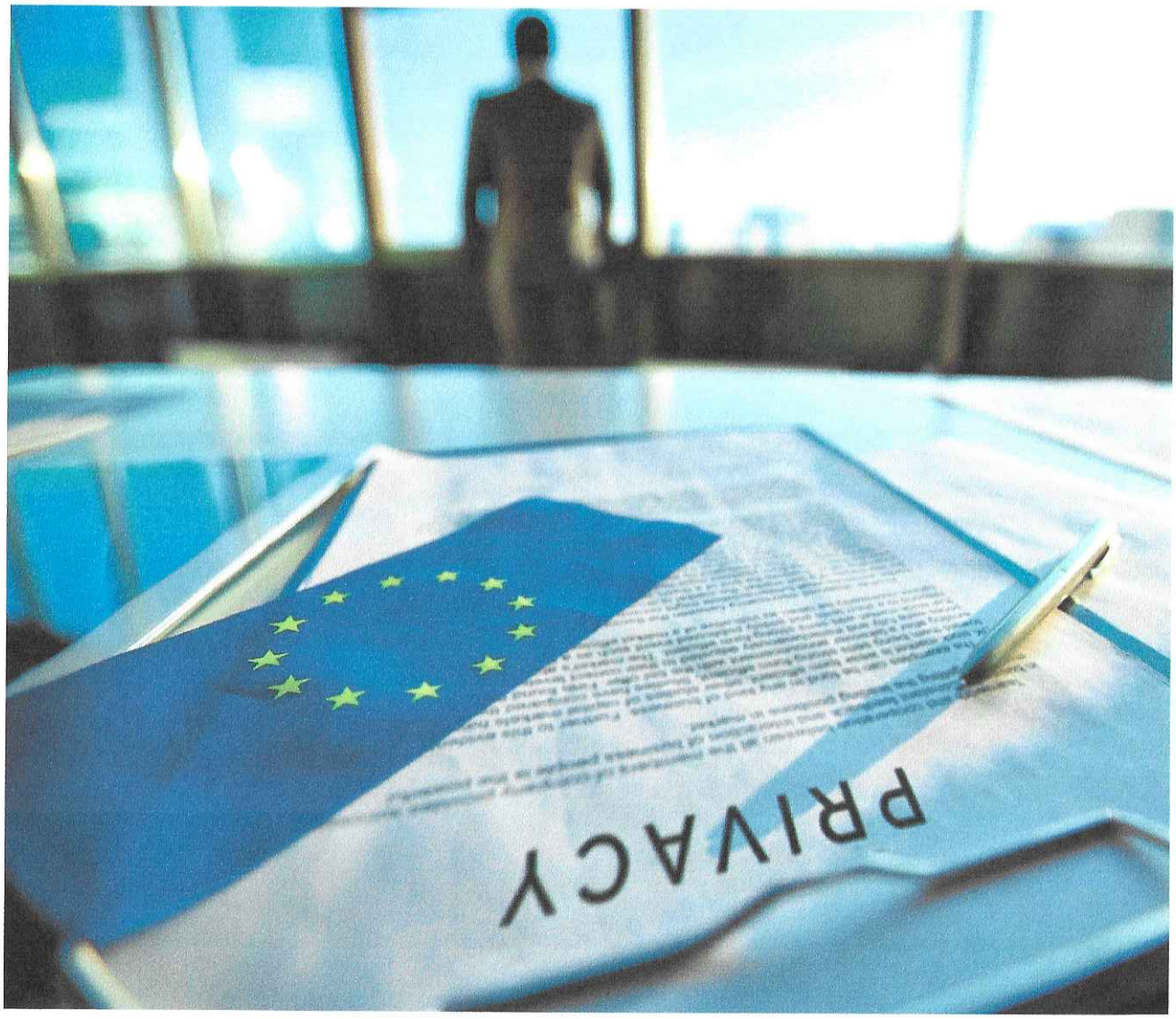
Responsabile del trattamento (da replicare laddove sia interno e/o esterno)	
Denominazione o ragione sociale	
Indirizzo	
Telefono	
Indirizzo email	
Riferimento lettera di incarico/contratto di servizi	

Responsabile della protezione dati _DPO	
Denominazione o ragione sociale	
Indirizzo	
Telefono	
Indirizzo email	
Riferimento eventuale contratto di servizi	

Incaricati dal Titolare o dal Responsabile del trattamento (da replicare per ogni finalità del trattamento)	
Nome e cognome	
Indirizzo	
Telefono	
Indirizzo email	
Riferimento eventuale contratto di servizi	

I DATI PERSONALI

La finalità del trattamento dati	La base giuridica del trattamento				
	Consenso	Esecuzione contratto	Adempimento obbligo di legge	Legittimo Interesse	Altro
1. Gestione dei dati del personale					
2. Gestione dei dati dei clienti e dei fornitori					
3. Dati sulla formazione del personale					
4. Dati sulla sicurezza sul lavoro					
5. Dati relativi alla gestione informatica					



LE FINALITÀ DEL TRATTAMENTO

1. GESTIONE DEI DATI DEL PERSONALE							
TIPOLOGIA DATI	• Dati identificativi • Dati particolari						
TIPOLOGIA DEL TRATTAMENTO	• Amministrazione gestione del personale	• Assunzioni - collaborazioni - dimissioni licenziamenti - provvedimenti disciplinari	• Iscrizione a sindacati • Inserimento in Registri cartacei ed elettronici	• Rilevazione e normalizzazione delle presenza	• Valutazione del personale	• Pagamento stipendi/ emolumenti	• Verifica congruità pagamento delle note spesa
CATEGORIA DI INTERESSATI	• Dipendenti dell'impresa	• Professionisti non dipendenti (consulenti, periti, assicuratori, revisori fiscali)					
DESTINATARI DEI DATI	• Personale interno	• Istituzioni • Autorità di Vigilanza	• Soggetti terzi (gestione contabilità e buste paga)	• Autorità giudiziaria			
TEMPI DI CONSERVAZIONE	• 10 anni o specificare eventuali altri termini						
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio			
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare tecnico	• accessi riservati al personale autorizzato	• protezione archivi informatici	• protezione fisica documenti	• backup • antivirus	• password	

2. GESTIONE DEI DATI DEI CLIENTI E DEI FORNITORI							
TIPOLOGIA DATI	• Dati personali/ identificativi dei referenti di clienti e fornitori	• Immagini personali	• Dati personali/ identificativi di clienti e fornitori	• CV Clienti e fornitori			
TIPOLOGIA DEL TRATTAMENTO	• Inserimento in registri	• Gestione rapporto commerciale (stipula contratti, invio corrispondenza)	• Utilizzo dati per fatturazione				
CATEGORIA DI INTERESSATI	• Clienti/Fornitori						
DESTINATARI DEI DATI	• Personale interno	• Autorità di Vigilanza					
TEMPI DI CONSERVAZIONE	• 10 anni						
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio			
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare tecnico						

3. DATI PERSONALI SULLA FORMAZIONE PROFESSIONALE DEL PERSONALE					
TIPOLOGIA DATI	• Dati personali/ identificativi	• Dati relativi al percorso professionale/ formativo	• Dati particolari (per esonero)	• Immagini personali anche tramite ripresa	
TIPOLOGIA DEL TRATTAMENTO	• Piani formativi	• Formazione • Formazione in materia di D.Lgs n. 231/2001	• Erogazione corsi formazione interna	• Gestione eventi formazione	• Relazione con soggetti terzi
CATEGORIA DI INTERESSATI	• Personale dipendente	• Soggetti terzi (professionisti coinvolti negli eventi formativi)			
DESTINATARI DEI DATI	• Personale Interno	• Soggetti terzi certificatori • Autorità di Vigilanza			
TEMPI DI CONSERVAZIONE	• Non determinato				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio	
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

4. DATI PERSONALI SULLA SICUREZZA SUL LAVORO (D.LGS. N. 81/2008 E S.M.)					
TIPOLOGIA DATI	• Dati personali/ identificativi	• Immagini personali anche tramite riprese	• Dati particolari	• Dati biometrici relativi alla salute (visibili solo da RIs e dal medico competente)	
TIPOLOGIA DEL TRATTAMENTO	• Visite mediche periodiche del personale	• Formazione del personale	• Adempimenti di cui al D.L.gs n. 81/2008	• Verifica dell'idoneità tecnico professionale dei dipendenti	
CATEGORIA DI INTERESSATI	• Personale dipendente				
DESTINATARI DEI DATI	• Medico competente	• Soggetti terzi certificatori	• Autorità di Vigilanza (Asl, Ispettorato lavoro, vigili del fuoco ecc.)	• Ente certificatore privato per la sicurezza	• RLS/RLST
TEMPI DI CONSERVAZIONE	• Non determinati				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio	
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

5. DATI RELATIVI ALLA GESTIONE INFORMATICA					
TIPOLOGIA DATI	• Dati personali/ identificativi	• Dati particolari			
TIPOLOGIA DEL TRATTAMENTO	• Gestione autorizzazione di accesso al sistema informatico	• Gestione attività per sicurezza, integrità e disponibilità dei dati trattati con mezzi automatizzati			
CATEGORIA DI INTERESSATI	• Personale dipendente	• Soggetti terzi (fornitori, operai iscritti alla Cassa, consulenti esterni)			
DESTINATARI DEI DATI	• Personale Interno	• Soggetti esterni che collaborano per la gestione del sistema informatico			
TEMPI DI CONSERVAZIONE	• 10 anni				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Accesso non autorizzato al sistema informatico	• Uso improprio	
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

6. CONTROLLI DI QUALITÀ					
TIPOLOGIA DATI	• Dati personali/ identificativi				
TIPOLOGIA DEL TRATTAMENTO	• Acquisizione dati previsti e indicati dallo standard internazionale sulla qualità (UNI EN ISO)	• Dati dipendenti e soggetti terzi impiegati nelle verifiche di conformità alle procedure per la formazione	• Comunicazione al Responsabile Qualità		
CATEGORIA DI INTERESSATI	• Personale dipendente	• Soggetti terzi (appalto, cooperativa esterna)	• Fornitori		
DESTINATARI DEI DATI	• Personale Interno	• Autorità di Vigilanza	• Clienti		
TEMPI DI CONSERVAZIONE	• 10 anni				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio	• Rischio specifico: divulgazione dati in grado di rilevare inadempienze
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

ALTRE VOCI DA AGGIUNGERE OVE ESISTENTI PER CIASCUNA FINALITÀ DI TRATTAMENTO

ANCE | ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

EDILSTAMPA
Marzo 2018