

ANCE

ASSOCIAZIONE NAZIONALE
COSTRUTTORI EDILI



PRIVACY

REGOLAMENTO UE n. 2016/679 SULLA PROTEZIONE DATI

BIANCA MARIA BARON & VALERIA ANDRETTA



www.ance.it



relazioniindustriali@ance.it



[@ancenazionale](https://twitter.com/ancenazionale)



Via Guattani 16 Roma



+39 06 84567 1



+39 06 84567 1



IL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI

GDPR – REG. UE n. 2016/679

E' APPLICABILE IN TUTTI GLI STATI MEMBRI DAL

25 MAGGIO 2018





**L'ADEGUAMENTO AL GDPR
NON PIU'COME UN COSTO MA COME UN INVESTIMENTO**



**PARITA' DI CONDIZIONI TRA LE IMPRESE NEL MERCATO
DELL'UNIONE**

**COMPLIANCE AL REGOLAMENTO COME NECESSITA'
PER LE IMPRESE**

**MAGGIORE PROTEZIONE E NUOVE OPPORTUNITA'
(*DATA BREACH*) ***



**MAGGIORE CONTROLLO DEGLI INTERESSATI SUI PROPRI
DATI PERSONALI (*DIRITTI*) ***

**CONFERIMENTO DEL POTERE DI INFLIGGERE SANZIONI
PECUNIARIE A TUTTE LE AUTORITA' DI CONTROLLO
(*GARANTE*)**



**MAGGIORE RESPONSABILIZZAZIONE DEL TITOLARE E
DEL RESPONSABILE DEL TRATTAMENTO**

**DIMOSTRAZIONE CHE IL TRATTAMENTO AVVIENE IN
CONFORMITA' CON IL GDPR *C.D. ACCOUNTABILITY***

**DA SISTEMA DI NOTIFICAZIONE
A SISTEMA DI *RESPONSABILIZZAZIONE***

COME?



DESIGNARE IL RESPONSABILE PROTEZIONE DATI (DPO) *

**SVOLGERE LA VALUTAZIONE DEL RISCHIO E LA VALUTAZIONE
D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) ***

PREDISPORRE IL REGISTRO DEI TRATTAMENTI *



MISURE DI PREVENZIONE:

PRIVACY BY DESIGN

DEFINIRE IL TRATTAMENTO IN COMPLIANCE CON IL GDPR,
DIMOSTRANDO DI AVER FATTO TUTTO PER EVITARE IL RISCHIO

PRIVACY BY DEFAULT

ADOTTARE TUTTI GLI STRUMENTI TECNOLOGICI PER PROTEGGERE IL DATO



DATO PERSONALE



QUALSIASI INFORMAZIONE RIGUARDANTE UNA PERSONA FISICA IDENTIFICATA O IDENTIFICABILE (*INTERESSATO*)



DATI ANAGRAFICI

DATI PARTICOLARI

NEW

- ✓ DATI RELATIVI ALLA SALUTE, ALL'APPARTENENZA SINDACALE, ETC... (EX DATI SENSIBILI)
- ✓ DATI GENETICI
- ✓ DATI BIOMETRICI

DATI PENALI

DATI CHE PRESENTANO RISCHI

NEW

DATI ANONIMI (SUI QUALI NON SI APPLICA IL GDPR)



ANONIMIZZAZIONE

NEW

QUANDO I DATI NON RICONDUCONO ALL'IDENTIFICAZIONE
DELL'INTERESSATO

NEW

PSEUDONIMIZZAZIONE

QUANDO I DATI NON RICONDUCONO ALL'INTERESSATO SE NON
CON L'UTILIZZO DI INFORMAZIONI AGGIUNTIVE



QUALSIASI OPERAZIONE COMPIUTA ANCHE SENZA L'AUSILIO DEI PROCESSI AUTOMATIZZATI

TIPOLOGIE DI TRATTAMENTO		
RACCOLTA	MODIFICA	RAFFRONTO
REGISTRAZIONE	ESTRAZIONE	INTERCONNESSIONE
ORGANIZZAZIONE	CONSULTAZIONE	LIMITAZIONE
STRUTTURAZIONE	USO	CANCELLAZIONE
CONSERVAZIONE	COMUNICAZIONE	DIFFUSIONE
ADATTAMENTO	MESSA A DISPOSIZIONE	DISTRUZIONE



PRINCIPI GENERALI DEL TRATTAMENTO

LICEITA' / CORRETTEZZA / TRASPARENZA

MINIMIZZAZIONE / PERTINENZA / PROPORZIONALITA'

LIMITAZIONE ALLA CONSERVAZIONE

SICUREZZA ED INTEGRITA'



DIRITTO DI INFORMAZIONE

DIRITTO DI ACCESSO

DIRITTO DI RETTIFICA

DIRITTO ALLA CANCELLAZIONE (C.D. ALL'OBLIO)

DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

DIRITTO ALLA PORTABILITA' DEI DATI

DIRITTO DI OPPOSIZIONE



GARANTE (AUTORITÀ DI CONTROLLO)

TITOLARE/CONTITOLARE

RESPONSABILE DEL TRATTAMENTO (ESTERNO)

INCARICATI

RESPONSABILE PROTEZIONE DATI (DPO)

NEW

INTERESSATI



DPO O «GARANTINO» COLUI CHE:

DIALOGA CON GLI INTERESSATI E CON L'AUTORITA' DI CONTROLLO ED E' INDIPENDENTE RISPETTO AL TITOLARE E AL RESPONSABILE

VALUTA I RISCHI DI OGNI TRATTAMENTO

SORVEGLIA LA CORRETTA OSSERVANZA DEL GDPR

N.B. DELL'INOSSERVANZA DEL GDPR SONO RESPONSABILI IL TITOLARE E IL RESPONSABILE



OBBLIGATORIO SE:

**IL TRATTAMENTO DEI DATI RICHIEDE UN MONITORAGGIO
REGOLARE E SISTEMATICO DEGLI INTERESSATI SU LARGA SCALA**

**SI EFFETTUANO TRATTAMENTI SU LARGA SCALA DI DATI
PARTICOLARI**

***IN TUTTI GLI ALTRI CASI
NON OBBLIGATORIO MA COMUNQUE CONSIGLIATO***



IN UN GRUPPO DI IMPRESE PUO' NOMINARSI ANCHE UN SOLO DPO PURCHE' SIA FACILMENTE RAGGIUNGIBILE DA CIASCUNA IMPRESA

DEVE FACILMENTE COLLOQUIARE CON L'AUTORITA' DI CONTROLLO E CON GLI INTERESSATI



DEVE ESSERE NOMINATO MEDIANTE UN ATTO DI DESIGNAZIONE CHE INDICHI TUTTE LE FUNZIONI AD ESSO ATTRIBUITE

LA SUA NOMINA DEVE POI ESSERE COMUNICATA ALL'AUTORITA' DI CONTROLLO



IDONEA QUALITÀ PROFESSIONALE

**CONOSCENZA DELLA NORMATIVA E DELLE PRASSI EUROPEE
IN MATERIA DI PROTEZIONE DEI DATI**

CONOSCENZA DEL GDPR

**CONOSCENZA DELLO SPECIFICO SETTORE DI ATTIVITÀ E
DELLA STRUTTURA ORGANIZZATIVA**



SORVEGLIA L'OSSERVANZA DEL GDPR

VALUTA I RISCHI DI OGNI TRATTAMENTO

**ASSISTE IL TITOLARE E IL RESPONSABILE NELLA REDAZIONE DEL
*REGISTRO DEI TRATTAMENTI***

COLLABORA CON IL TITOLARE PER LA CONDUZIONE DELLA *DPIA*

FACILITATORE, PUNTO DI CONTATTO, FIGURA DI GARANZIA



OGNI TITOLARE E OGNI RESPONSABILE DEL TRATTAMENTO *TENGONO* IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO SVOLTE SOTTO LA PROPRIA RESPONSABILITÀ

NON E' PRESCRITTA UNA FORMA OBBLIGATORIA DI REGISTRO



È OBBLIGATORIO

- ✓ PER LE IMPRESE CON PIÙ DI 250 DIPENDENTI
- ✓ IN TUTTI I CASI IN CUI IL TRATTAMENTO INCLUDA DATI PARTICOLARI, NONCHE' PENALI
- ✓ IN TUTTI I CASI CHE POTREBBERO PROVOCARE RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

ANCHE QUANDO NON È OBBLIGATORIO È COMUNQUE SEMPRE CONSIGLIATO (*ACCOUNTABILITY*)



IL REGISTRO CONTIENE:

I DATI DI CONTATTO DEL TITOLARE, DEL RESPONSABILE E DEGLI ALTRI SOGGETTI INCARICATI	LE MISURE DI SICUREZZA ADOTTATE
LE FINALITA' DEL TRATTAMENTO	LA TIPOLOGIA DEL TRATTAMENTO
LA BASE GIURIDICA DEL TRATTAMENTO	LE CATEGORIE DEI DESTINATARI
LE CATEGORIE DEI DATI	I TEMPI DI CONSERVAZIONE DEI DATI
I DESTINATATI DEI DATI	I RISCHI SPECIFICI INERENTI I DATI



PUO' CONTENERE ANCHE ALTRI DATI RELATIVI A:

PAESE DI PROVENIENZA E DI DESTINAZIONE DEI DATI	UFFICIO DI RIFERIMENTO DEI SINGOLI TRATTAMENTI
ADESIONE AD UN CODICE DI CONDOTTA	VALUTAZIONE DEL RISCHIO
ADESIONE AD UN MECCANISMO DI CERTIFICAZIONE	VALUTAZIONE DI IMPATTO DPIA



I SOGGETTI

TITOLARE/CONTITOLARE	
DENOMINAZIONE O RAGIONE SOCIALE	
INDIRIZZO	
TELEFONO	
INDIRIZZO E-MAIL	



I SOGGETTI



RESPONSABILE DEL TRATTAMENTO/RAPPRESENTANTE/DPO

DENOMINAZIONE O RAGIONE SOCIALE

INDIRIZZO

TELEFONO

INDIRIZZO E-MAIL

RIFERIMENTO LETTERA DI INCARICO/CONTRATTO DI SERVIZI



FINALITA' DEL TRATTAMENTO	FONDAMENTI DI LICEITA' DEL TRATTAMENTO				
	CONSENSO	ESECUZIONE CONTRATTO	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					



1. GESTIONE DEI DATI DEL PERSONALE

TIPOLOGIA DEI DATI	<ul style="list-style-type: none">• dati identificativi• dati particolari
TIPOLOGIA DEL TRATTAMENTO	<ul style="list-style-type: none">• amministrazione del personale• iscrizione ai sindacati• pagamento stipendi/emolumenti• rilevazione presenze• pagamento note spese
CATEGORIA DI INTERESSATI	<ul style="list-style-type: none">• dipendenti dell'impresa• professionisti non dipendenti (consulenti, periti, assicuratori, revisori fiscali)
DESTINATARI DEI DATI	<ul style="list-style-type: none">• personale interno• soggetti terzi (contabilità, buste paga)• Istituzioni• Autorità di Vigilanza• Autorità giudiziarie
TEMPI DI CONSERVAZIONE	<ul style="list-style-type: none">• 10 anni o diversi termini
RISCHI SPECIFICI INERENTI I DATI	<ul style="list-style-type: none">• perdita• distruzione• divulgazione non autorizzata• uso improprio
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	<ul style="list-style-type: none">• disciplinare tecnico• protezione fisica dei documenti• accesso riservato al personale autorizzato• protezione archivi informatici• backup• antivirus• password



CONSENSO



ESECUZIONE DI UN CONTRATTO

ADEMPIMENTI AD OBBLIGHI DI LEGGE

SALVAGUARDIA DEGLI INTERESSI VITALI DELL'INTERESSATO

ESECUZIONE DI UN COMPITO DI INTERESSE PUBBLICO

LEGITTIMO INTERESSE



INFORMATO *(PROCEDUTO DALL'INFORMATIVA)*

SPECIFICO *(CHIARO E ESPLICITO PER CIASCUNA FINALITA' DEL TRATTAMENTO)*

CONSAPEVOLE *(ATTO POSITIVO ED INEQUIVOCABILE)*

LIBERO *(SVINCOLATO DA COSTRIZIONI E CON POSSIBILITA' DI REVOCA)*

**NECESSARIO IN ASSENZA
DELLE ALTRE CONDIZIONI DI LICEITA'**



**ISPIRATA AL PRINCIPIO DI TRASPARENZA
(CHIARA, INTELLEGIBILE E CONCISA)**

NECESSARIA SEMPRE ANCHE IN ASSENZA DI CONSENSO

**IN QUALUNQUE FORMA PURCHE' COMPROVABILE
(ACCOUNTABILITY)**



TEMPI DI CONSEGNA DELL'INFORMATIVA:

- ✓ **AL MOMENTO DELLA RACCOLTA DEI DATI**
- ✓ **ENTRO UN MESE, SE RACCOLTI PRESSO TERZI**



E' OBBLIGATORIA

**QUANDO IL TRATTAMENTO PRESENTA UN RISCHIO ELEVATO
PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE**

**E' COMUNQUE CONSIGLIATA LA DEFINIZIONE DELLA DPIA
ANCHE SE NON SI RAVVISANO I GRAVI RISCHI PRESCRITTI
DALLA NORMA**



**IN CASO DI VIOLAZIONE DEI DATI PERSONALI
CON RISCHIO DI VIOLAZIONE DEI DIRITTI E
DELLE LIBERTA' FONDAMENTALI DELLE PERSONE**



**OBBLIGO DI NOTIFICA ALL'AUTORITA' DI CONTROLLO
ENTRO 72 ORE E NOTIFICA ALL'INTERESSATO
QUANDO IL RISCHIO E' ELEVATO**



È VOLONTARIA

**NON RIDUCE LA RESPONSABILITÀ DEL TITOLARE O
DEL RESPONSABILE DEL TRATTAMENTO**

**PUÒ ESSERE RILASCIATA DALL'AUTORITA' DI CONTROLLO O DA ALTRI
ENTI CERTIFICATORI ACCREDITATI**

HA UNA VALIDITÀ DI 3 ANNI

E' RINNOVABILE E REVOCABILE PER PERDITA DEI REQUISITI



**IL TITOLARE E' RESPONSABILE PER IL DANNO CAUSATO
DAL SUO TRATTAMENTO**

**IL RESPONSABILE RISPONDE SOLO SE NON HA ADEMPIUTO
AGLI OBBLIGHI PREVISTI DAL GDPR**

**TITOLARE E RESPONSABILE SONO TENUTI AL RISARCIMENTO
DEL DANNO**

SANZIONI AMMINISTRATIVE E PECUNIARIE:

- ✓ € 10.000.000 O, PER LE IMPRESE, FINO AL 2% DEL FATTURATO MONDIALE TOTALE ANNUO
- ✓ € 20.000.000 O, PER LE IMPRESE, FINO AL 4% DEL FATTURATO MONDIALE TOTALE ANNUO
(PER SPECIFICHE VIOLAZIONI)





IL CONTROLLO DEI LAVORATORI, TRAMITE IMPIANTI AUDIOVISIVI E ALTRI STRUMENTI DI CONTROLLO A DISTANZA, E' CONSENTITO SOLO PER:

- ✓ **ESIGENZE ORGANIZZATIVE E PRODUTTIVE**
- ✓ **PER LA SICUREZZA DEL LAVORO**
- ✓ **PER LA TUTELA DEL PATRIMONIO AZIENDALE**



SOLO PREVIO ACCORDO COLLETTIVO:

- ✓ **STIPULATO DA RSU O DA RSA**
- ✓ **STIPULATO DALLE ASSOCIAZIONI SINDACALI NAZIONALI PER IMPRESE IN DIVERSE PROVINCE DELLA STESSA REGIONE O IN PIÙ REGIONI**

IN MANCANZA DI ACCORDO:

- ✓ **PREVIO AUTORIZZAZIONE DELLA SEDE TERRITORIALE DELL'INL**
- ✓ **PREVIO AUTORIZZAZIONE DELLA SEDE CENTRALE DELL'INL PER IMPRESE DISCLOCATE IN DIVERSI AMBITI TERRITORIALI**



ACCORDO NON RICHIESTO:

- ✓ **PER GLI STRUMENTI UTILIZZATI DAL LAVORATORE E PER SVOLGERE ATTIVITA' LAVORATIVA**
- ✓ **PER GLI STRUMENTI DI REGISTRAZIONE DI ACCESSI E PRESENZE**

NOTA INL N. 299/2017: SOLO IN ASSENZA DEI LAVORATORI, SENZA POSSIBILITÀ DI CONTROLLO "PRETERINTENZIONALE" SUL PERSONALE

NOTA INL N. 5/2018: CHIARIMENTI SULL' UTILIZZO DI TELECAMERE, DI SISTEMI DI VIDEOSORVEGLIANZA BASATI SU TECNOLOGIE DIGITALI E SUL TRATTAMENTO DEI DATI BIOMETRICI





GRAZIE

Bianca Maria Baron

baronbm@ance.it

Valeria Andretta

andrettav@ance.it