LINEE GUIDA PRIVACY
per il settore delle costruzioni

GDPR

ANCE | ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

Legacoop PRODUZIONE & SERVIZI

CNA Costruzioni

ANAEPA Confartigianato Edilizia

LINEE GUIDA PRIVACY

PER IL SETTORE DELLE COSTRUZIONI

Progetto interassociativo Ance, Legacoop Produzione e Servizi,
CNA Costruzioni, Anaepa Confartigianato
per l'attuazione del Regolamento UE 679/2016 - RGPD nel settore delle costruzioni

a cura di **Dino Bogazzi** e **Giuliano Marullo**

settembre 2021

ANCE - Via G.A. Guattani, 16 - 00161 Roma
www.ance.it

LEGACOOP Produzione e Servizi - Via G.A. Guattani, 9 - 00161 Roma
www.lps.coop

CNA Costruzioni - Piazza Mariano Armellini, 9 A - 00162 Roma
www.cna.it

ANAEPA Confartigianato - Via di San Giovanni in Laterano, 152 - 00184 Roma
www.anaepa.it

Su iniziativa di

ANCE ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

Associazione nazionale cooperative di produzione lavoro e servizi legacoop PRODUZIONE & SERVIZI

ANAEPA Confartigianato Edilizia

CNA Costruzioni

Presentazione delle Linee Guida Privacy del settore edile
Roma 14 marzo 2024

Sala degli Atti parlamentari della Biblioteca "Giovanni Spadolini"

presso il Senato della Repubblica

Ore 11:00 — **Saluti istituzionali**

Federica BRANCACCIO
Presidente Ance Associazione Nazionale Costruttori Edili

Enzo PONZIO
Presidente CNA Costruzioni

Ore 11:30 — **Presentazione delle Linee Guida Privacy Edilizia**

Ing. Giuliano MARULLO
Curatore delle Linee guida

Ore 12:00 — **Il punto di vista dell'Autorità Garante della Privacy**

Dott. Francesco MODAFFERI
Direttore Dipartimento Realtà Economiche e Produttive
Garante per la Protezione dei Dati Personali

Ore 12:30 — **Saluti conclusivi**

Stefano CRESTINI
Presidente Confartigianato ANAEPA Edilizia

Andrea LAGUARDIA
Direttore Legacoop Produzione e Servizi

Le opinioni e i contenuti espressi nell'ambito dell'iniziativa sono nell'esclusiva responsabilità dei proponenti e dei relatori e non sono riconducibili in alcun modo al Senato della Repubblica o ad organi del Senato medesimo

L'accesso alla sala - con abbigliamento consono e, per gli uomini, obbligo di giacca e cravatta - è consentito fino al raggiungimento della capienza massima

I lavori del convegno saranno trasmessi in diretta streaming al link https://webtv.senato.it e sul canale YouTube del Senato Italiano https://www.youtube.com/user/SenatoItaliano.

1 INTRODUZIONE

1.1 Caratteristiche dimensionali e produttive delle imprese del settore delle costruzioni in Italia

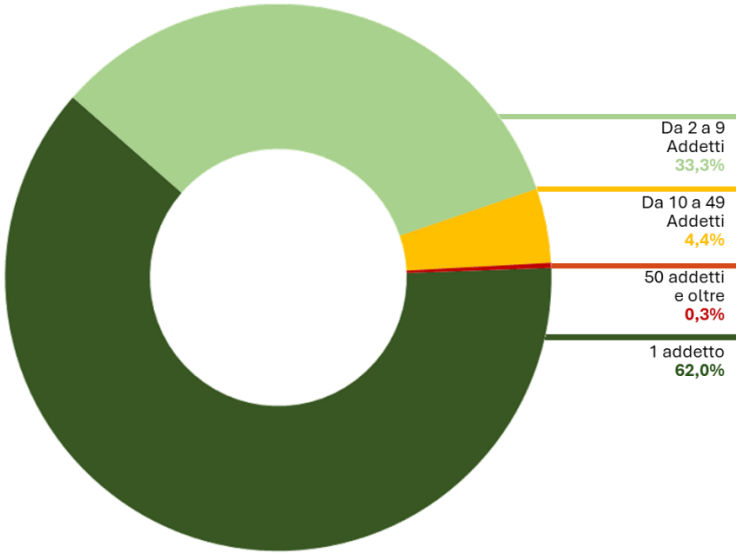
Ricordiamo, per avere un riferimento condiviso, le definizioni di micro, piccola, media e grande impresa adottate dalla Commissione Europea, basate sul numero di dipendenti e sulla dimensione economica:

- **micro impresa**: azienda con un numero di dipendenti inferiore alle 10 unità e che realizza un fatturato o un bilancio annuo uguale o inferiore ai 2 milioni di euro;
- **piccola impresa**: azienda con meno di 50 occupati e un fatturato o bilancio annuo non superiore ai 10 milioni di euro;
- **media impresa**: azienda con un massimo di 250 unità lavorative e un fatturato inferiore o uguale ai 50 milioni di euro o un totale di bilancio annuo non superiore ai 43 milioni di euro;
- **grande impresa**: azienda con più di 250 unità lavorative o un fatturato superiore ai 50 milioni di euro o un totale di bilancio annuo superiore ai 43 milioni di euro;

ANCE[1] nell'ottobre 2022 ha aggiornato la ormai tradizionale analisi annuale della struttura produttiva delle imprese di costruzioni italiane, documento dal quale sono state tratte le tabelle e le considerazioni riportate nel seguito.

Ripartizione per classe di addetti:

Le caratteristiche dimensionali delle imprese di costruzione mostrano una polverizzazione molto pronunciata, con oltre il 60% delle imprese (316mila su 512mila) rappresentato da realtà con un unico addetto. Un ulteriore terzo (ovvero 172mila imprese) si concentra nella fascia 2-9 addetti. Le imprese medie (10-49 addetti – 23mila imprese) e le grandi (50 addetti e oltre – 1.540 imprese) hanno quote contenute (4,4% e 0,3%. La dimensione media delle imprese nel settore si attesta sui 2,8 addetti ad impresa, molto ridotta se confrontata ai 10,4 addetti per l'industria in senso stretto e ai 3,5 per i servizi (3,9 addetti per l'intero sistema produttivo industriale e dei servizi).



Riconducendo i dati delle imprese italiane alle classi dimensionali adottate dalla Commissione Europea, la ripartizione risulta sostanzialmente la seguente: micro imprese: 95,3%, piccole imprese: 4,4%, medie e grandi imprese: 0,3%, con le grandi imprese stimabili in poche decine di unità (sono di norma quelle che operano in modo rilevante anche all'estero).

Ripartizione per classe di fatturato

[1] Fonte: ANCE, Osservatorio congiunturale sull'industria delle costruzioni, Gennaio 2024

Il settore delle costruzioni risulta inoltre caratterizzato da una elevata quota di imprese con volumi d'affari molto ridotti. L'86% delle imprese di costruzione dichiara di avere un fatturato inferiore ai 500 mila euro.

1.2 Il progetto interassociativo Linee guida Privacy

La realtà del settore delle costruzioni, già esaminata nel paragrafo precedente, ha stimolato le Associazioni di rappresentanza a predisporre una strumentazione che, nel rispetto del Regolamento Europeo 679/2016 – RGPD (Regolamento generale sulla protezione dei dati), potesse semplificare e rendere meno oneroso il percorso che ciascuna impresa deve compiere per adempiere agli obblighi derivanti dal regolamento stesso.

La numerosità dei soggetti potenzialmente interessati (oltre 500.000) - e la valutazione che i processi produttivi delle imprese del settore delle costruzioni non presentano in ogni caso una elevata criticità in tema di protezione dei dati personali - hanno portato momentaneamente ad escludere la predisposizione di un Codice di Condotta ex articolo 40 del RGPD; tale strumento comporta per le Associazioni l'obbligo di costituire uno specifico Organismo di Monitoraggio con le caratteristiche descritte nell'art. 41 dello stesso RGPD e meglio dettagliate nel successivo documento *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* emesso dall'European Data Protection Board – EDPB nel mese di giugno 2019.

ANCE, Legacoop Produzione e Servizi, CNA Costruzioni e Anaepa Confartigianato hanno pertanto deciso di sviluppare delle Linee Guida; in particolare il progetto è stato caratterizzato nel modo seguente:

È stato predisposto un set di documenti standard già adattati alle caratteristiche del settore delle costruzioni:

- informative, contratti per responsabili, designazioni ed autorizzazioni.
- registro dei Trattamenti;
- policy aziendale per l'utilizzo dei sistemi informatici da parte dei designati ed autorizzati.
- alcune Procedure che possono servire come base di riferimento (gestione delle violazioni, esercizio dei diritti, ecc.);
- documentazione relativa a specifici trattamenti (Videosorveglianza, geolocalizzazione, ecc.).

Sono stati sviluppati specifici approfondimenti per i trattamenti di dati personali che maggiormente caratterizzano le imprese del settore delle costruzioni:

- comunicazione dei dati dei dipendenti di aziende che operano in appalto/subappalto al committente/appaltatore, con la finalità di far fronte alla responsabilità solidale contributiva e retributiva di cui all'art. 29 del D.Lgs n. 276/2003, quando previsto contrattualmente;
- comunicazione di una particolare tipologia di dati sanitari (prescrizioni limitative all'esercizio di una mansione) ai responsabili operativi dei cantieri, al fine di tutelare la salute e la sicurezza dei lavoratori;
- videosorveglianza dei cantieri mobili;
- geolocalizzazione dei mezzi di cantiere.

Tali documenti sono oggi disponibili alle imprese attraverso i siti web od altre piattaforme delle singole Associazioni e possono essere dalle stesse imprese liberamente scaricati e ulteriormente personalizzati.

Sono state predisposte le presenti Linee Guida, che contengono ed illustrano tutto il lavoro svolto e tutto il materiale reso disponibile alle imprese.

Sono state programmate Iniziative di promozione delle Linee Guida Privacy da parte di tutte le Associazioni di settore.

Il Regolamento 679/2016 – RGPD prevede la possibilità di individuare misure semplificate di applicazione per le micro, piccole e medie imprese. Per poter effettuare un lavoro rigoroso, nella

predisposizione delle Linee Guida Privacy per il settore delle costruzioni sono state fatte alcune ipotesi semplificative:

- l'impresa di costruzioni considerata è di dimensione micro o piccola;
- l'impresa svolge esclusivamente attività di costruzione;
- l'impresa non lavora, neanche occasionalmente, all'estero;
- l'impresa non trasferisce dati personali fuori della Unione Europea;
- la strumentazione ICT dell'azienda è limitata.

Le imprese che si riconoscono in queste ipotesi (definite imprese standard), possono adottare quanto suggerito dalle Linee Guida, limitando al massimo le personalizzazioni.

Le Linee Guida hanno in ogni caso predisposto per le imprese standard un ventaglio di soluzioni, articolando più in dettaglio le ipotesi semplificative elencate in precedenza (per esempio in funzione della effettiva strumentazione ICT).

Le imprese che non si riconoscono in una o più delle ipotesi alla base delle Linee Guida debbono approfondire in modo autonomo le problematiche conseguenti tale aspetto, integrando e/o modificando quanto proposto dalle stesse Linee Guida.

Il Tavolo Tecnico incaricato di predisporre le Linee Guida Privacy interassociative aveva sostanzialmente completato il lavoro nel mese di dicembre 2019 e i primi mesi del 2020 erano stati destinati alla revisione finale e all'editing di quanto predisposto.

Si prevedeva, a seguire, la presentazione del testo finale delle Linee Guida Privacy all'Autorità Garante per la protezione dei dati personali e di organizzare un evento interassociativo per la diffusione dello strumento alle imprese associate.

La pandemia causata dal Covid-19 ha reso più complesse le attività di revisione finale che, comunque, si sono concluse nel febbraio 2022. Successivamente, anche a seguito di interlocuzioni con l'Autorità Garante, è stato ritenuto opportuno apportare ulteriori revisioni, da ultimo a seguito dell'introduzione, con il D.Lgs. n.24 del 10 marzo 2023, delle disposizioni riguardanti la protezione delle persone che segnalano violazioni.

Il presente documento è stato condiviso con l'Autorità Garante nella sua impostazione generale.

1.3 Il gruppo di lavoro per la redazione delle Linee Guida Privacy

Il progetto, nato nel 2018 per iniziativa di ISTECO[2], è stato coordinato da Dino Bogazzi, con il supporto, in qualità di esperto della materia, di Giuliano Marullo.

Il Tavolo Tecnico ha consentito un confronto fra le quattro Associazioni sull'impostazione generale e sui singoli elaborati. Componenti del Tavolo Tecnico interassociativo, su designazione delle singole Associazioni, sono:

- Dino Bogazzi, coordinatore del progetto
- Giuliano Marullo
- Valeria Andretta, ANCE
- Myriam Buffoni, Legacoop Produzione e Servizi
- Danilo Caspoli e Claudio Buganza, per CNA Costruzioni
- Federica Colombini, Anaepa Confartigianato

Il documento finale, dopo l'approvazione del Tavolo Tecnico, è stato ulteriormente validato da un secondo tavolo interassociativo al quale hanno partecipato:

- Beatrice Sassi, rappresentante di ANCE
- Marco Mingrone, rappresentante di Legacoop Produzione e Servizi
- Riccardo Masini, rappresentante di CNA Costruzioni
- Daniela Scaccia, rappresentante di Anaepa Confartigianato

[2] L'Istituto per lo Sviluppo Tecnologico nelle Costruzioni – ISTECO, in precedenza Istituto Certificazione qualità Imprese e servizi per le Costruzioni - ICIC, ha operato fino a tutto il 2021.

Soci di ISTECO nel 2018, al momento del lancio del presente progetto, erano le cinque maggiori associazioni di categoria del settore delle costruzioni:

- ANCE – Associazione Nazionale Costruttori Edili, aderente a Confindustria
- Legacoop Produzione e Servizi
- CNA Costruzioni – Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa
- ANAEPA Confartigianato Edilizia
- OICE – Associazione delle Organizzazioni italiane di Ingegneria, architettura e Consulenza tecnico-Economica, aderente a Confindustria

A questi si aggiungono come soci di diritto, fin dalla fondazione dell'Istituto, i tre Ministeri di riferimento per il settore delle costruzioni: Ministero Infrastrutture e Trasporti, Ministero dello Sviluppo Economico e Ministero dei Beni e delle Attività Culturali e del Turismo.

2 LINEE GUIDA PER LA GESTIONE DEI DATI PERSONALI PER LE IMPRESE DI COSTRUZIONE

2.1 Premessa

Il 9 settembre 2018 è entrato in vigore il DLgs 101/18 “Disposizioni di adeguamento della normativa nazionale alle disposizioni del RGPD” che ha modificato il DLgs 196/03 “Codice in materia di protezione dei dati personali” evidenziando, fra l’altro, l’esigenza di individuare misure semplificate di applicazione per le micro, piccole e medie imprese.

Le presenti Linee Guida hanno lo scopo di fornire un supporto proprio alle micro, piccole imprese del settore delle costruzioni italiano.

Per poter effettuare un lavoro rigoroso, nella predisposizione delle presenti Linee Guida sono state formulate alcune ipotesi per identificare l’azienda “standard” alla quale sono rivolte:

- L’impresa di costruzioni considerata è di dimensione micro o piccola.
- L’impresa svolge esclusivamente attività di costruzione.
- L’impresa non lavora, neanche occasionalmente, all’estero.
- L’impresa non trasferisce dati personali fuori della Unione Europea.
- La strumentazione ICT dell’azienda è limitata.
- L’impresa non utilizza sistemi decisionali o di monitoraggio integralmente automatizzati.

Le imprese che si riconoscono in queste ipotesi possono adottare quanto suggerito dalle Linee Guida, limitando al massimo le personalizzazioni.

Le imprese che non si riconoscono in una o più delle ipotesi alla base delle Linee Guida debbono approfondire in modo autonomo le problematiche conseguenti tale aspetto, integrando e/o modificando quanto proposto dalle stesse Linee Guida.

2.2 Il Regolamento generale sulla protezione dei dati

Il RGPD o regolamento generale sulla protezione dei dati (Regolamento UE n. 2016/679), è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy; tale regolamento è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed è entrato in vigore dal 25 maggio 2018.

Scopo del regolamento è quello di rafforzare ed uniformare all'interno dell'Unione Europea la protezione dei dati personali dei cittadini e dei residenti.

Dalla sua entrata in vigore, il RGPD ha sostituito i contenuti della precedente direttiva UE sulla protezione dei dati; l'Italia si è adeguata alla normativa europea con il DLgs 101 del 10 agosto 2018.

Il RGPD disciplina esclusivamente il trattamento dei dati personali delle persone fisiche mentre sono esclusi dall'applicazione del codice i dati delle persone giuridiche, degli enti e delle associazioni.

Nel seguito vengono date alcune sintetiche e non esaustive indicazioni sul RGPD (rivolte soprattutto alle "imprese standard"), ritenute utili per una miglior comprensione dei contenuti delle presenti Linee Guida (fra parentesi quadre sono riportati i riferimenti agli articoli del RGPD relativi)[3].

Le categorie di dati tutelati

I dati personali tutelati dal RGPD sono classificabili in tre macro categorie:

- *Dati personali* in genere: informazioni di diversa natura relative ad una persona fisica identificata o comunque identificabile.
- *Dati personali particolari* (o *sensibili* secondo una precedente definizione): origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati relativi alla vita sessuale o all'orientamento sessuale, dati genetici, biometrici o relativi alla salute [Art. 9].
- *Dati personali relativi a condanne penali o reati:* il trattamento di questi dati deve avvenire sotto il controllo dell'autorità pubblica o se è autorizzato dal diritto dell'Unione che deve prevedere garanzie appropriate per i diritti e le libertà degli interessati [Art. 10].

Gli attori del RGPD

Il RGPD identifica le figure competenti alle quali è consentito trattare i dati personali [Art. 4]:

a. **Interessato**: è la persona fisica a cui si riferiscono i dati personali.
b. **Titolare del trattamento**: è la persona fisica, la persona giuridica, la Pubblica Amministrazione o qualsiasi altro ente a cui è consentito determinare le finalità e le modalità del trattamento dei dati personali. Possono esistere casi di contitolarità del trattamento (e in questo caso i contitolari devono fare un accordo che disciplina il modo in cui vengono svolte specifiche operazioni. L'interessato può esercitare i diritti previsti dal RGPD nei confronti di e contro ciascun titolare)
c. **Persona autorizzata** (in precedenza definita Incaricato) al trattamento dei dati personali: è la persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di gestione dei dati.
d. **Responsabile del trattamento**: è la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente che tratta i dati per conto del titolare del trattamento.
e. **Destinatario del trattamento**: è la persona fisica, la persona giuridica, la Pubblica Amministrazione o qualsiasi altro ente che riceve comunicazione di dati personali dal titolare del trattamento.
f. **Terzi**: sono tutti coloro che non sono identificati come interessati, titolari, responsabili, autorizzati al trattamento.

[3] Nell'ambito delle iniziative previste dalla strategia 2021-2023 dell'European Data Protection Board per promuovere la sensibilizzazione alla normativa in materia di privacy è stata pubblicate una guida (https://edpb.europa.eu/sme-data-protection-guide/home_en#home-title) per aiutare le piccole e medie imprese a conformarsi alla normativa in materia di protezione dei dati personali con l'obiettivo di fornire informazioni pratiche alle PMI sulla conformità al RGPD in un formato accessibile e facilmente comprensibile (attualmente in lingua inglese ma traducibile con i normali strumenti forniti dai browser).

Le Responsabilità per il trattamento dei dati personali

Il trattamento di dati personali illecito può comportare l'insorgere di una molteplicità di responsabilità: amministrativa, civile e penale.

La responsabilità civile comporta una valutazione ex ante del livello di rischio ed una sostanziale inversione dell'onere della prova.

Per non rispondere del danno derivante da un inadeguato trattamento dei dati personali (nell'ambito della responsabilità civile) occorre provare di aver fatto tutto il possibile per evitarlo; di fatto, quella sanzionata dal RGPD è una colpa in organizzazione che può essere evitata solo analizzando il rischio ed implementando un sistema gestionale per la privacy (identificazione dei responsabili, assegnazione di responsabilità, formazione, informative, registro dei trattamenti, procedure, ecc.) congruente con le prescrizioni del RGPD e le caratteristiche dell'impresa.

Relativamente alla responsabilità amministrativa derivante dalla violazione della disciplina di protezione dei dati, il compito di controllare che i trattamenti di dati personali siano conformi al RGPD nonché alle leggi e ai regolamenti nazionali è affidato all'*Autorità Garante per la Protezione dei dati*.

Tale Autorità ha anche il compito di esaminare i reclami e prescrivere, ove necessario, ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui.

Nel caso rilevi trattamenti che violano le disposizioni del RGPD, il Garante può:

- rivolgere ammonimenti al titolare o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento;
- imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento;
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento;
- imporre sanzioni pecuniarie che, nei casi più gravi, possono avere un importo fino al 4% del fatturato annuo dell'impresa

Liceità del trattamento

Il trattamento dei dati personali è lecito solo se ricorre **almeno una** delle seguenti condizioni [Art. 6]:

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

Il trattamento dei dati appartenenti a categorie particolari di dati personali (che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché quando il trattamento riguarda dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) è vietato a meno che non si verifichi uno dei casi seguenti *(di seguito vengono riportati quelli di maggiore intesse per una impresa di costruzioni)* [Art. 9]:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un

contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale.

Si noti che il trattamento di dati appartenenti alle categorie particolari non può essere legittimato, a differenza di quanto previsto per gli altri dati, dalla necessità di eseguire un contratto o dal legittimo interesse del titolare.

Consenso

Quando il trattamento è basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il consenso al trattamento dei propri dati personali [Art. 7 e 8].

Il RGPD non prescrive la forma del consenso che, quindi, potrebbe anche essere orale; dovendo però essere verificabile, in caso di necessità è responsabilità del titolare dimostrare di aver proceduto correttamente.

In ogni caso, per l'ottenimento di un consenso *conforme* è una "dichiarazione o un'azione positiva inequivocabile". Per i dati personali **particolari** il consenso deve essere **esplicito**, cioè, l'interessato deve fornire una dichiarazione esplicita di consenso.

L'interessato deve poter revocare il proprio consenso in ogni momento e con la stessa facilità con la quale lo ha espresso e il titolare dovrà sospendere le attività di trattamento interessate.

È necessario che il consenso sia liberamente prestato ma questa libertà non risulta dimostrabile, di regola, all'interno dei rapporti di lavoro, a causa dell'asimmetria di potere presente nell'ambito dell'occupazione (si veda l'Appendice C).

Trasparenza

Il RGPD prevede che il titolare del trattamento debba sempre fornire agli interessati, prima del trattamento, le informazioni sulle finalità e le modalità dei trattamenti che intende effettuare, ciò alla luce del principio di trasparenza (art. 5 par. 1 lett. a) del Regolamento) In particolare, gli artt. 13 e 14 del Regolamento, distinguendo trai dati raccolti presso l'interessato e i dati raccolti presso altri soggetti, individua il contenuto minimo dell'informativa. [Art. 13 e 14].

Diritti degli interessati

Il RGPD riconosce all'interessato una molteplicità di diritti [Artt. da 15 a 22], tra i quali, quello di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardi (può richiedere una copia dei dati che lo riguardano purché questo non leda i diritti o la libertà altrui), di richiedere la rettifica dei dati relativi a sé o, in molti casi, la loro cancellazione o la limitazione dei trattamenti.

L'interessato ha diritto di opporsi ai trattamenti che si basano sul legittimo interesse del titolare.

Sicurezza dei dati

Il titolare del trattamento e il responsabile del trattamento debbono garantire la sicurezza dei dati raccolti, mettendo in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato 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 [Art. 32].

Violazione dei dati

La violazione dei dati personali (Data Breach) [Art. 33] è definita come la violazione di sicurezza che comporta accidentalmente o in modo illecito la distribuzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Un Data Breach può essere la conseguenza di un evento doloso (esempio un attacco informatico) o accidentale (banalmente, la semplice perdita di una chiavetta USB o l'invio di dati personali ad un indirizzo errato).

In presenza di un evento di questa natura, il titolare del trattamento dei dati ha l'obbligo legale di comunicarlo (entro 72 ore da quando ne è venuto a conoscenza) all'Autorità Garante per la Privacy a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

Se la violazione dei dati può avere delle conseguenze gravi, il titolare ha l'obbligo di avvertire tempestivamente anche gli interessati [art. 34 RGPD].

2.3 Contenuti e organizzazione delle Linee Guida

Vista la rapida evoluzione delle tecnologie informatiche ed il loro sempre più generalizzato utilizzo in tutte le aziende del settore delle costruzioni il trattamento dei dati personali viene svolto prevalentemente in formato digitale e le misure di sicurezza richieste per la protezione dei dati personali si integrano alle buone pratiche per il trattamento di tutti i dati aziendali.

> *Su questi temi ogni Associazione ha già fornito strumenti e supporti per i propri associati e non saranno trattate in queste Linee Guida.*

Nella gestione dei dati personali elemento essenziale è la trasparenza nei confronti degli interessati che devono sapere quali loro dati personali sono trattati, per quali finalità, da chi, con quali modalità e chi potrà venirne a conoscenza. L'interessato deve, inoltre, essere informato dei propri diritti relativamente ai trattamenti effettuati sui propri dati e come può esercitarli.

> *Queste Linee Guida analizzano le problematiche relative alle INFORMATIVE (Vedi Cap. 4.1) e forniscono numerosi esempi dai quali i titolari possono prendere spunto per garantire la trasparenza dei trattamenti.*

Il titolare del trattamento dei dati deve assicurare che i dati personali siano trattati unicamente da personale che agisca sotto la sua autorità (espressamente autorizzato e formato) o da responsabili (che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato) che operano in base ad un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

> *Nelle Linee Guida sono analizzate le modalità per procedere alla DESIGNAZIONE degli autorizzati (vedi Cap. 4.2) e per stipulare ACCORDI CON I RESPONSABILI ai quali sono affidati trattamenti per conto del titolare (vedi Cap. 4.3).*
>
> *Sono stati predisposti anche documenti e procedure per istruire gli autorizzati ed alcune procedure (Vedi Cap. 4.5).*

Ogni titolare del trattamento deve analizzare e registrare, nel Registro dei trattamenti, le attività di trattamento svolte sotto la propria responsabilità e, in alcuni casi particolari, quando un tipo di

trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, può dover effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

In queste Linee Guida sono illustrate le caratteristiche che deve avere un REGISTRO DEI TRATTAMENTI e presentati degli esempi di trattamenti di valenza generale (vedi Cap. 4.4).

Sono anche fornite alcune indicazioni per la gestione di trattamenti particolari a partire dalle VALUTAZIONI DI IMPATTO (vedi Cap. 4.6).

Queste Linee Guida sono state progettate utilizzando un approccio "stratificato" per permettere una rapida lettura da parte del titolare dell'impresa del settore delle costruzioni che potrà avere una indicazione di massima sulle prescrizioni della normativa per la protezione dei dati personali e potrà selezionare le tipologie di documenti da produrre per i trattamenti che effettua nella propria attività.

Per ogni tipologia di documenti troverà le informazioni sui modelli predisposti e i facsimili del modello di base e di alcune varianti già parzialmente personalizzate. Dovrà scegliere il documento che più si avvicina alle proprie esigenze e completare la personalizzazione.

Nelle Appendici possono essere trovati i riferimenti normativi e le indicazioni fornite dalle autorità europee o nazionali. La lettura delle Appendici può servire a chiarire eventuali dubbi in fase di personalizzazione. Il contenuto delle Appendici sarà anche utilizzato come base di riferimento per le attività di formazione che le varie Associazioni svolgeranno sul tema della protezione dei dati personali per supportare i propri associati (per questo motivo sono stati mantenuti i riferimenti ai documenti originali ai quali il formatore potrà attingere per una trattazione più completa).

Utilizzo delle Linee Guida

Le Linee Guida consentono una lettura "stratificata". Il titolare può infatti leggerle trovando un sempre maggiore livello di dettaglio:

Nel Capitolo 4 viene fornita una prima illustrazione delle tipologie di documenti predisposti nelle presenti Linee Guida all'interno delle quali il titolare può individuare quelli di interesse.

Il titolare può trovare, nel Capitolo 5, una illustrazione di dettaglio delle caratteristiche dei documenti predisposti relativi alle varie tipologie. All'interno delle varianti proposte il titolare può quindi trovare quella più vicina alle proprie esigenze.

Nelle APPENDICI sono riportati, per le varie tipologie, i riferimenti normativi e le indicazioni fornite dai garanti europei. Il titolare interessato può quindi approfondire i vari aspetti di interesse.

I FACSIMILI dei documenti sono disponibili in formato elettronico attraverso le applicazioni fornite dalle varie Associazioni.

Necessità di personalizzazione dei documenti

I FACSIMILI devono essere analizzati e personalizzati rispetto alle specifiche caratteristiche dell'azienda.

Nei documenti vengono evidenziate, con una barra sulla destra, le parti per le quali la personalizzazione è:

Barra Verde: Opportuna.

Barra Rossa: Fortemente consigliata o addirittura obbligatoria.

Analoghe indicazioni sono fornite dalle applicazioni per i documenti in formato digitale.

Utilizzo dei facsimili

Ogni azienda, in funzione delle proprie caratteristiche, dovrà scegliere fra i vari facsimili proposti quelli di interesse.

Di seguito è riportato uno schema di sintesi dell'utilizzo atteso dei vari facsimili in base alle caratteristiche dell'azienda.

	Impresa "standard" senza personale.	Impresa "standard" con personale, anche part-time, in cantiere.	Impresa "standard" con personale, anche part-time, in ufficio.	Impresa "standard" con personale sia in cantiere che in ufficio.
Informativa Base	X	X	X	X
Informativa ai Dipendenti / Collaboratori		X	X	X
Informativa per i Lavoratori di altre imprese impegnate nei Cantieri		X		X
Informativa ai Clienti / Fornitori	X	X	X	X
Informativa per i Curricula		X	X	X
Informativa per le Mail			X	X
Informativa per il Sito aziendale				X
Designazione Referente Base				X
Designazione Referente per il Sistema Informativo				X
Designazione Referente Privacy				X
Designazione Base			X	X
Designazione Autorizzato al trattamento			X	X
Designazione RSPP / Collegio Sindacale / Organismo di Vigilanza				X
Accordo Base – Solo Clausole	X	X	X	X
Accordo Base – Solo Allegati	X	X	X	X
Descrizione trattamento: Amministrazione del personale		X	X	X
Descrizione trattamento: Gestione Contabile	X	X	X	X
Descrizione trattamento: Manutenzione dei sistemi informatici	X	X	X	X
Descrizione trattamento: Manutenzione dei pacchetti software gestionali			?	?
Descrizione trattamento: Distributore di software SAAS			?	?
Descrizione trattamento: Amministratori di sistema			?	?
Policy e Prescrizioni per gli autorizzati al trattamento dei dati				X
Procedura per incidenti di sicurezza dei dati e delle violazioni	X	X	X	X
Procedura per l'esercizio dei diritti	X	X	X	X
Procedura per la gestione del personale		X	X	X
Procedura e Valutazione per l'utilizzo di dispositivi video		?	?	?
Procedura e valutazione per la geolocalizzazione		?	?	?

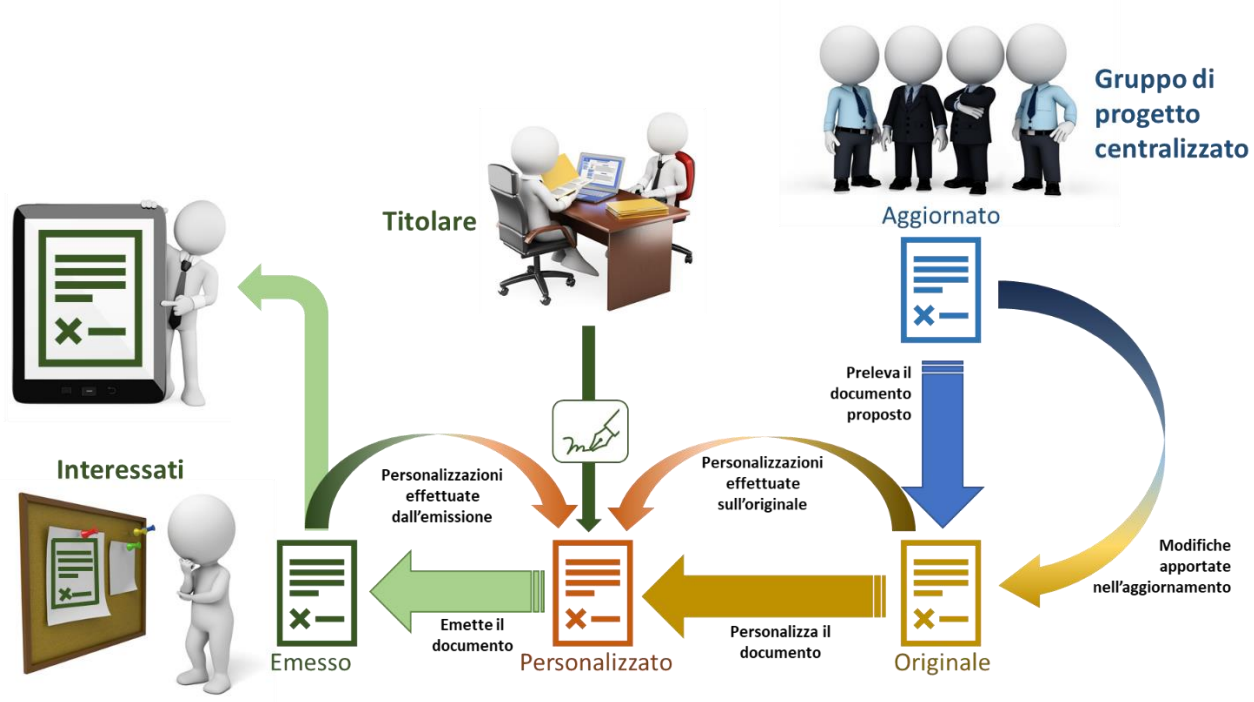
Applicazioni software per la gestione dei documenti predisposti

Per l'effettiva fruizione dei documenti predisposti si prevede l'utilizzo di appositi software messi a disposizione dalle varie Associazioni.

Il titolare potrà, attraverso il software messo a disposizione dalla propria Associazione, accedere ai documenti in formato elettronico per selezionare i documenti di interesse ed apportare tutte le personalizzazioni opportune.

Il titolare, attraverso il software utilizzato, potrà mettere i documenti desiderati (informative, valutazioni d'impatto, ecc.) a disposizione di tutti gli interessati via WEB consentendo l'accesso da qualunque dispositivo (dal cellulare al PC) e fornendo anche una traduzione automatica dei documenti nelle varie lingue.

I software messi a disposizione dalle varie Associazioni sono predisposti per seguire gli aggiornamenti che, il gruppo di lavoro che ha prodotto le presenti Linee Guida e che proseguirà l'attività di supporto alle imprese del settore, apporterà ai documenti a seguito di indicazioni scaturite dal loro concreto utilizzo.



Le ultime versioni aggiornate sono sempre disponibili dagli applicativi ("**Aggiornato**"). Il titolare può scegliere il documento di interesse ed ottenerne una copia ("**Originale**").

A questo punto il titolare apporterà le modifiche alle parti da personalizzare evidenziate dal programma ("**Personalizzato**") e, conclusa l'operazione, potrà emettere ufficialmente il documento ("**Emesso**").

Se il documento è di quelli da pubblicare sul WEB con l'emissione sarà immediatamente visibile da tutti gli interessati.

A fronte di una modifica apportata dal gruppo di progetto interassociativo al documento ("**Aggiornato**") verrà evidenziata la modifica al titolare e gli aspetti significativi verranno evidenziati nelle note di revisione.

Il titolare, presa visione delle modifiche apportate centralmente (rispetto al documento "**Originale**" in base al quale aveva lavorato) potrà recepirle apportando le modifiche al documento aziendale ("**Personalizzato**") e, una volta concluse le correzioni, potrà procedere alla nuova emissione ("**Emesso**"), indicando le principali modifiche apportate e, ovviamente, modificando la data di emissione.

Per facilitare le operazioni di aggiornamento l'applicazione fornisce, in ogni momento, l'informazione sulle modifiche a suo tempo effettuate sul documento originale.

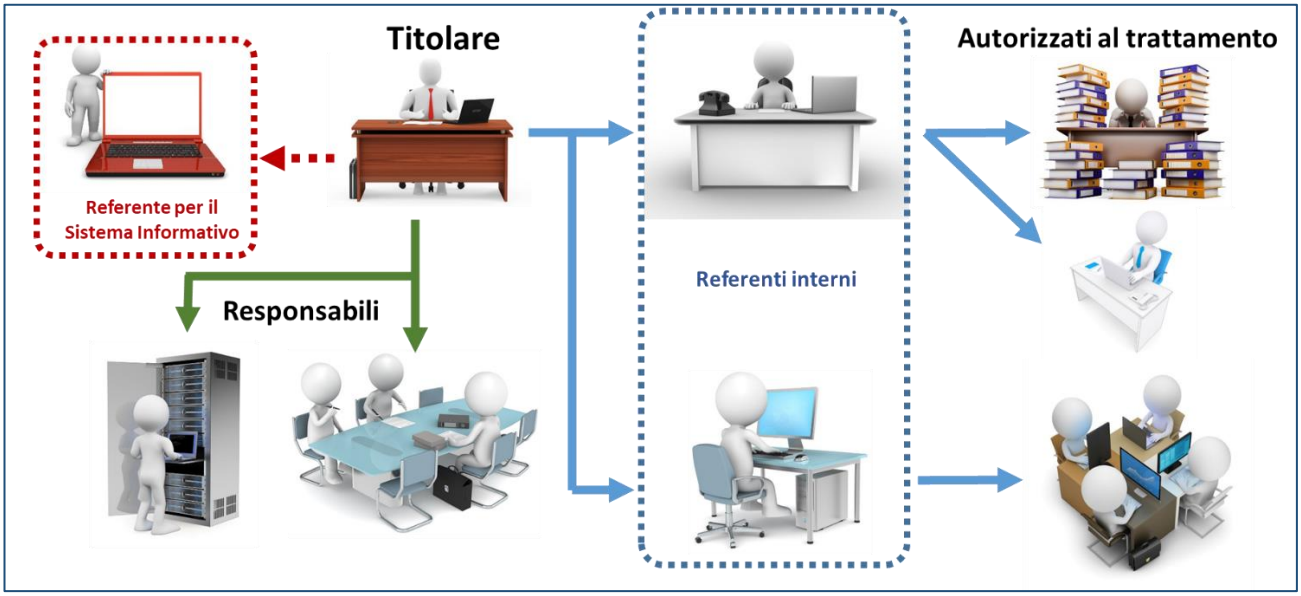
Prima di emettere il documento il titolare può prendere visione delle modifiche che verranno apportate in caso di emissione.

Ogni interessato potrà, accedendo tramite il link presente nel sito dell'azienda o accedendo direttamente all'applicazione e utilizzando la Partita Iva dell'azienda, visualizzare tutti i documenti "pubblicati".

Soggetti previsti

Il Regolamento europeo 2016/679 "Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (d'ora in poi **RGPD**) prevede le seguenti categorie di soggetti:

Per l'azienda "standard" oggetto delle presenti Linee Guida sono state considerate come significative le sole figure riportate con colore rosso secondo lo schema sotto riportato.



Il **Titolare** è colui che deve mettere in atto misure tecniche e organizzative adeguate per proteggere i dati.

Il Titolare deve designare come **Autorizzati** chi tratta i dati personali.

Il Titolare deve stipulare un contratto con i **Responsabili** che trattano dati personali per suo conto.

In alcune aziende il Titolare può designare dei ***Referenti interni*** che coordinano le attività degli Autorizzati.

In alcune aziende il Titolare può farsi affiancare da un ***Referente per il sistema informativo*** che, in genere, si interfaccerà a sua volta con gli specialisti IT eventualmente nominando un Responsabile Tecnico del Sistema Informatico.

2.4 Le Tipologie dei Documenti

Le informative

Uno degli aspetti principali del corretto trattamento dei dati personali è la trasparenza nei confronti degli interessati.

Particolare attenzione deve, quindi, essere posta alla predisposizione delle informative.

Nell'Appendice A "Linee Guida sulla Trasparenza" sono riportati gli articoli del RGPD di maggiore interesse e descritte le caratteristiche che devono avere le informative con le specificità correlate al settore delle costruzioni.

Ogni trattamento può essere effettuato solo se rispetta il principio di liceità. Per l'impresa standard le condizioni che rendono lecito il trattamento sono generalmente legate, salva comunque la necessità di avere riguardo al caso di specie, all'esecuzione di un contratto, al rispetto di obblighi di legge, all'assolvimento di obblighi in materia di diritto del lavoro e di medicina del lavoro, ai diritti in sede giudiziaria per contenziosi in atto o in situazioni precontenziose. È necessario in ogni caso, affinché il trattamento sia conforme alla legge, che, oltre al principio di liceità del trattamento, siano rispettati gli altri principi di protezione dei dati (principi di correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza).

Le condizioni di liceità sono illustrati nell'Appendice B.

In alcuni casi il trattamento può avvenire sulla base del consenso espresso dall'interessato ma a condizione che questo sia dimostrabile, chiaro, revocabile e liberamente prestato (si ricorda che il consenso dei dipendenti, di norma, non può essere ritenuto una idonea condizione di liceità, salvo in casi particolari).

Nell'Appendice C sono analizzate le caratteristiche che deve avere il consenso.

In alcuni casi il trattamento di dati (non appartenenti a categorie particolari) può essere legittimato dal perseguimento del legittimo interesse del titolare del trattamento o di terzi.

A questo aspetto è dedicata l'Appendice D.

Nel capitolo "**5.1 - Informative**" sono illustrate le caratteristiche della informativa di base che è stata predisposta e che ogni titolare deve personalizzare per ottenere le varie informative per i vari interessati. Per facilitare il lavoro del titolare sono illustrate alcune varianti già parzialmente personalizzate sulle quali il titolare dovrà intervenire con le personalizzazioni residue inevitabilmente legate alle specifiche problematiche e modalità aziendali.

NOTA BENE: Fra le varianti viene presentata anche la "Informativa per i Lavoratori di altre imprese impegnate nei Cantieri" progettata per tutta la filiera delle costruzioni.

Designazioni

Fondamentale per il corretto trattamento dei dati personali è l'individuazione di chi, all'interno dell'azienda o comunque sotto l'autorità del titolare, può trattare i dati.

È necessario individuare con precisione i compiti di ogni soggetto, curarne l'istruzione e formalizzare l'autorizzazione al trattamento.

*Nell'Appendice E "Designati" sono riportati gli articoli del RGPD e del Decreto Legislativo 169/03 "Codice in materia di protezione dei dati personali" (d'ora in poi "**Codice**") di maggiore interesse in relazione alle designazioni.*

Nel capitolo **"5.2 – Designazioni"** è illustrata la designazione di base sia per i referenti (significative per imprese più strutturate) che per i semplici autorizzati. Ogni titolare deve valutare quali designazioni sono opportune per la propria realtà e personalizzare i documenti di base. Per facilitare il lavoro del titolare sono state predisposte alcune varianti, illustrate sempre nello stesso capitolo, già parzialmente personalizzate sulle quali il titolare dovrà intervenire con le personalizzazioni residue inevitabilmente legate alle specifiche problematiche e modalità aziendali.

Responsabili del trattamento

Molto spesso il titolare (anche e soprattutto per piccole aziende) decide di far effettuare un trattamento per suo conto da un responsabile (*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*).

In questi casi deve assicurarsi che il responsabile presenti garanzie sufficienti per il corretto trattamento dei dati personali e stipulare un apposito contratto.

Nell'Appendice F "Titolare e Responsabile" è riportato l'articolo del RGPD che disciplina i rapporti con i responsabili e vengono fornite indicazioni su come attribuire correttamente i ruoli di titolare e responsabile e sulle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7.

Nel capitolo **"5.3 - Accordi per il trattamento dei dati con il Responsabile"** è illustrato l'accordo di base predisposto sulla base delle "clausole contrattuali tipo" che ogni titolare deve personalizzare per ottenere i vari accordi per i vari responsabili. Per facilitare il lavoro del titolare sono state illustrate anche alcune varianti già parzialmente personalizzate relativamente alle descrizioni dei trattamenti sulle quali il titolare dovrà intervenire con le personalizzazioni residue inevitabilmente legate alle specifiche problematiche e modalità dell'affidamento del trattamento.

Registro dei trattamenti

È opportuno che il titolare analizzi i trattamenti di dati personali dallo stesso effettuati.

Il Registro dei trattamenti previsto dal RGPD è un valido strumento per una prima analisi dei trattamenti.

Nell'Appendice G "Registro delle attività di trattamento" è riportato l'articolo del RGPD che lo disciplina e i riferimenti al Registro semplificato proposto dal Garante italiano.

Nel capitolo **"5.4 - Registro dei trattamenti"** sono riportati i contenuti del registro semplificato per le imprese di costruzione che ogni titolare deve compilare con i trattamenti specifici. Per facilitare il lavoro del titolare viene proposto un esempio di Registro con esempi dei principali trattamenti soprattutto rivolti a chi gestisce il personale.

Policy e Procedure

Il titolare deve fornire agli autorizzati precise indicazioni su come operare.

Nell'Appendice H "Trattamento dei dati personali dei lavoratori" sono riportate alcune indicazioni fornite dal Garante in ambito lavorativo.

Nel capitolo **"5.5 – Policy e Procedure"** viene illustrato il documento predisposto per fornire le disposizioni aziendali per chi tratta le informazioni aziendali.

In caso di violazioni dei dati personali sono richieste al titolare una serie di attività.

Nell'Appendice I "Violazioni" sono riportati gli articoli del RGPD che le disciplinano.

Nel capitolo **"5.5 – Policy e Procedure"** viene illustrato il documento predisposto per la gestione degli incidenti.

Il titolare deve essere pronto a rispondere ad un interessato che desideri esercitare i propri diritti.

Nell'Appendice J "Diritti" sono riportati gli articoli del RGPD che li disciplinano.

Nel capitolo **"5.5 – Policy e Procedure"** viene illustrato il documento predisposto per permettere agli interessati di esercitare i propri diritti.

Il titolare dovrà porre una particolare attenzione per il trattamento dei dati del personale.

Nel capitolo **"5.5 – Policy e Procedure"** viene illustrata la procedura per la gestione del personale" che analizza vari aspetti anche molto specifici legati ai trattamenti legati alle nuove tecnologie.

Trattamenti specifici

Al ricorrere di determinate circostanze il titolare, prima di procedere al trattamento, deve effettuare una valutazione dell'impatto.

Nell'Appendice K "Valutazioni d'impatto" è riportato l'articolo del RGPD che le disciplina e una indicazione sui trattamenti da sottoporre alla valutazione d'impatto.

Nel capitolo **“5.6 – Trattamenti specifici”** vengono illustrati i documenti predisposti per particolari trattamenti (Videosorveglianza, Geolocalizzazione, Gestione delle segnalazioni).

2.5 Documenti di base e varianti

Informative

Documento Base (Inf_00)

Come previsto dall'Art. 12 del RGPD "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro".

A tal fine è stata predisposta una Informativa che contiene le seguenti sezioni:

- Identità e dati di contatto del Titolare del trattamento [Art. 13 1a, 1b – Art. 14 1a, 1b].
- Finalità del trattamento cui i dati sono destinati i dati personali e relativa base giuridica [Art. 13 1c, 1d, 2c, 2e – Art. 14 1c, 2b, 2d, 2f].
- Categorie di dati personali trattati [Art. 14 1d].
- Categorie di destinatari dei dati personali [Art. 13 1e – Art. 14 1e].
- Modalità del trattamento.
- Principi generali [Art. 13 1f, 2f – Art. 14 1f, 2g].
- Periodo di conservazione dei dati personali [Art. 13 2a - Art. 14 2a].
- Diritti esercitabili [Art. 13 2b, 2d – Art. 14 2c, 2e].

È quindi prevista la raccolta degli eventuali consensi.

Fra i destinatari dei dati personali sono previsti tutti i soggetti terzi che svolgono attività per conto del Titolare: Titolari autonomi, Contitolari e Responsabili esterni. Sarà cura del Titolare tenere e rendere disponibile su richiesta dell'interessato l'elenco completo.

Varianti

Informativa ai Dipendenti (Inf_01)

Organizzazione

Per facilitare la lettura si è scelto di riportare inizialmente una sintesi del documento con i rimandi alle varie sezioni successive.

L'informativa richiama la "Informativa per il trattamento dei dati nei rapporti di lavoro" (vedi avanti) che deve essere a disposizione dei dipendenti.

Soggetto

Per facilitare la comprensione del testo si è preferito usare l'espressione "lavoratori" piuttosto che una forma pronominale di cortesia.

Consenso

"Data la dipendenza risultante dal rapporto datore di lavoro/dipendente, è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto. … Per la maggior parte delle attività di trattamento svolte sul posto di lavoro, la base legittima non può e non dovrebbe essere il consenso del dipendente in considerazione della natura del rapporto tra datore di lavoro e dipendente" [Linea Guida sul consenso].

Nella informativa proposta non si prevede la necessità di raccogliere il consenso del lavoratore.

Finalità del trattamento

Il provvedimento del Garante per la protezione dei dati personali del 5 giugno 2019 [9124510] prevede che il trattamento dei dati appartenenti categorie particolari può essere effettuato solo se necessario:

- per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti collettivi anche aziendali, ai sensi del diritto interno, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro (art. 88 del Regolamento UE 2016/679), nonché del riconoscimento di

agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale;

- anche fuori dei casi di cui al punto precedente, in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
- per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo;
- per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose; resta salvo quanto stabilito dall'art. 60 del Codice;
- per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
- per garantire le pari opportunità nel lavoro;

per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

Dati trattati per il legittimo interesse del titolare.

Il perseguimento del legittimo interesse del datore di lavoro[4] permette di trattare i dati per:

- comunicare i dati anagrafici e curricula dei lavoratori ad altre aziende per la preparazione di gare o per l'esecuzione di lavori in associazione temporanea;
- controllare le spese sostenute per esami medici;
- annotare i periodi di utilizzo da parte del personale dei veicoli aziendali (ad esempio per poter attribuire la responsabilità in caso di violazioni al codice della strada).

Si ritengono, infatti, gli interessi del datore di lavoro tali da non intaccare i diritti e le libertà fondamentali dei lavoratori.

Nel caso di trattamenti effettuati in base al legittimo interesse, è opportuno che, nell'informativa ai lavoratori, venga ricordato il loro diritto ad opporsi ai suddetti trattamenti per motivi connessi alla propria situazione particolare.

Nel caso di ulteriori specifici trattamenti dovrà essere aggiunta una apposita sezione che descrive i trattamenti con le indicazioni relative alla legittimità (soprattutto per il rispetto dello Statuto dei Lavoratori) e il riferimento ai Test di Bilanciamento effettuati.

Vengono quindi descritte le categorie di dati trattati.

Categorie di dati particolari trattati

Nell'informativa è prevista una sezione nella quale al lavoratore è evidenziato come alcuni dati che potrebbe fornire potrebbero permettere di ricavare informazioni appartenenti a categorie particolari.

Dati personali forniti dal lavoratore relativamente ad altri soggetti

L'Art.14 1.d prevede che all'interessato vengano indicate le categorie di dati raccolti quando questi non sono forniti direttamente dall'interessato.

Nell'informativa è previsto che il Dipendente possa fornire dati di altri soggetti (es. familiari). In questi casi dovrà comunicare alle persone fisiche titolari di detti dati i contenuti essenziali dell'informativa ed informarli dei Loro diritti e, qualora necessario, ottenerne preventivamente il consenso.

Destinatari

Sono previsti come destinatari, specificatamente in relazione alla filiera delle costruzioni, anche:

- enti bilaterali.

[4] Il gruppo interassociativo ha predisposto una bozza di test di bilanciamento che permette di valutare che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato. Ogni impresa dovrà personalizzarlo in riferimento ai propri specifici trattamenti.

Dati Personali trattati dal lavoratore

Per i lavoratori autorizzati a trattare i dati sono previste delle specifiche designazioni (vedi avanti).

Qualunque lavoratore potrebbe però accedere, anche involontariamente, a dati personali trattati dal Titolare. Per questo è stata prevista, all'interno dell'informativa, anche una sezione relativa agli obblighi di riservatezza.

Conservazione dei dati.

Tutti i dati personali, ed in particolare quelli appartenenti a categorie particolari, possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi di legge o per perseguire le finalità definite. A tal fine è opportuno, anche mediante controlli periodici, verificare costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione deve essere prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

Attribuzione delle responsabilità del Medico Competente

Come ribadito dal Garante della protezione dei dati personali nel documento "Il ruolo del 'medico competente' in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale" del 14/5/21 [9585367]: "… il medico non tratta i dati per conto del datore di lavoro ma, in qualità di titolare del trattamento (artt. 4, n. 7 e 24 del Regolamento), in base a specifiche diposizioni di legge finalizzate anzitutto al perseguimento dell'interesse pubblico di tutela della salute nei luoghi di lavoro e della collettività.

Stante la titolarità del trattamento dei dati del medico competente (artt. 4, n. 7 e 24 del Regolamento), essendo questo l'unico legittimato a trattare i dati sanitari dei lavoratori indispensabili per lo svolgimento della funzione di protezione della salute e sicurezza dei luoghi di lavoro, gli eventuali flussi di dati personali tra il datore di lavoro e il medico competente devono intendersi quali "comunicazioni" di dati personali (cfr. la definizione contenuta all'art. 2-ter, par. 4, lett. a) del Codice), i cui presupposti sono rinvenibili nel richiamato quadro normativo di settore".

Nell'incarico al Medico Competente dovrà quindi essere inserito un paragrafo del tipo:

Il Medico tratterà tutti i dati oggetto del presente incarico in qualità di Titolare autonomo per tutte le fasi del processo (pianificazione delle visite, richiesta di analisi, raccolta dei risultati delle analisi, ecc.) che potranno essere svolte direttamente dal Medico o da Suoi incaricati o da altre Società con le quali lo stesso dovrà stipulare un contratto ai sensi dell'Art. 28 del RGPD. Sarà compito del Medico fornire una informativa ai sensi dell'Art.14 del RGPD agli interessati relativamente al trattamento dei dati.

In ogni caso il Medico è obbligato alla riservatezza anche relativamente alle altre informazioni, diverse dai dati sanitari, delle quali potrebbe venire a conoscenza, ad esempio, nell'analisi del DVR e nella partecipazione alle Riunioni periodiche per la sicurezza.

La Legge 3 luglio 2023, n 85 "Conversione in legge, con modificazioni, del decreto-legge 4 maggio 2023, n. 48, recante misure urgenti per l'inclusione sociale e l'accesso al mondo del lavoro" ha apportato modifiche alla sostituzione del Medico Competente (non è più previsto l'incarico da parte del Datore di Lavoro al quale verrà comunicato Art. 14) e alla consegna della cartella sanitaria e di rischio alla fine del rapporto di impiego ("in occasione della visita medica preventiva o della visita medica preventiva in fase preassuntiva di cui all'articolo 41, richiede al lavoratore di esibire copia della cartella sanitaria e di rischio rilasciata alla risoluzione del precedente rapporto di lavoro e ne valuta il contenuto ai fini della formulazione del giudizio di idoneità, salvo che ne sia oggettivamente impossibile il reperimento").

Informativa ai Dipendenti che operano nei Cantieri (Inf_01a)

L'informativa è identica a quella per tutti i Dipendenti ma in più prevede la possibilità che i dati vengano forniti anche:

- a responsabili di cantieri presso i quali il lavoratore potrebbe operare;

- a Committenti/Appaltatori nell'ambito di contatti di Appalto/Subappalto (ad esempio per assolvere agli oneri derivanti dalla gestione della sicurezza nei cantieri D.Lgs. 81/2008 e/o dalla responsabilità solidale ex art. 29 del D.Lgs. n. 276/2003).

In particolare, i dati del lavoratore (anche "particolari" quali ad esempio le prescrizioni che accompagnano le idoneità) devono essere forniti unicamente ai responsabili dei cantieri presso i quali il lavoratore opera. In casi particolari, come ad esempio nei lavori di manutenzione stradale o lavori che necessitano di esecuzione immediata per prevenire incidenti, per organizzare misure di salvataggio o per garantire continuità nell'erogazione di servizi essenziali per la popolazione, nei quali il lavoratore può essere impiegato, con minimo preavviso, presso cantieri geograficamente vicini, è possibile valutare la necessità di fornire detti dati anche ai responsabili dei cantieri presso i quali il Lavoratore potrebbe operare (per un bilanciamento fra i diritti alla protezione dei dati personali e la salute e sicurezza dei lavoratori).

Il lavoratore che opera nei cantieri viene informato di come vengono garantiti i suoi dati personali nelle comunicazioni fra Subappaltatore, Appaltatore e Committente.

Informativa per la Trasparenza (Inf_01b)

Nel caso in cui vengano utilizzati sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni, nonché indicazioni incidenti sulla sorveglianza, la valutazione, oltre che le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori è stata predisposta una informativa di base che dovrà essere personalizzata in base alle informazioni ricavabili dalla Valutazione d'impatto (obbligatoria).

Informativa ai Collaboratori (Inf_02)

L'informativa ai Collaboratori è analoga a quella per i Dipendenti escluse le specificità legate al rapporto di lavoro.

Informativa ai Collaboratori che operano nei Cantieri (Inf_02a)

Anche per i Collaboratori è prevista una specifica informativa per quelli che operano nei Cantieri analoga a quanto visto per i Dipendenti.

Informativa per i Lavoratori di altre imprese impegnate nei Cantieri (Inf_03)

Per provvedere alla gestione della sicurezza nel Cantiere D.Lgs 81/2008 e per permettere la corretta gestione dalla responsabilità solidale ex art. 29 del D.Lgs. n. 276/2003 ogni impresa che opera in un Cantiere Edile deve comunicare i dati personali dei propri lavoratori impegnati nel cantiere all'appaltatore che poi li dovrà comunicare al Committente ed al Coordinatore per la sicurezza.

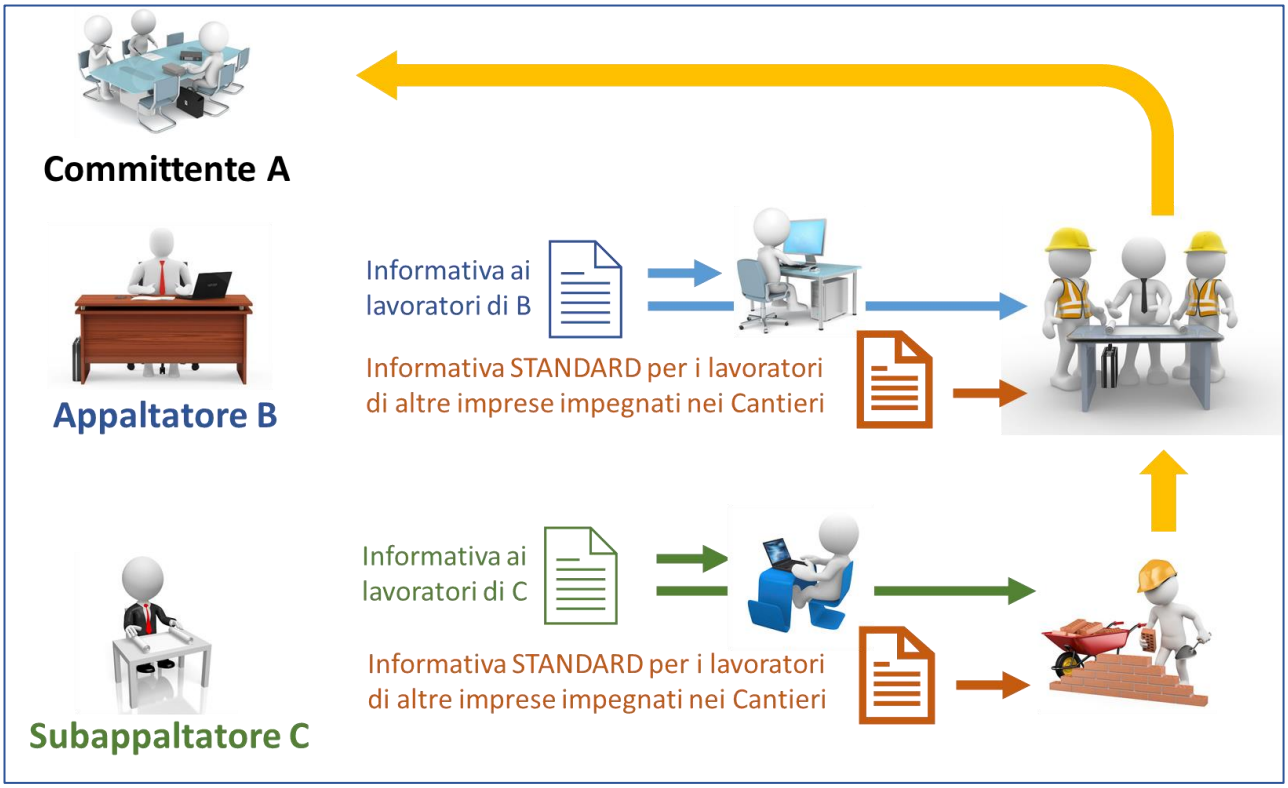
In particolare, potrebbero essere trasmessi i dati riferiti alla retribuzione e alla contribuzione del lavoratore (es. buste paga), nonché quelli relativi alle idoneità che, qualora contengano delle prescrizioni potrebbero rilevare lo stato di salute del lavoratore.

In alcuni casi le Imprese devono fornire al Committente i contatti di alcuni dipendenti, ad esempio, in caso di reperibilità per manutenzioni.

Detti dati, consegnati in esecuzione di un obbligo contrattuale, vengono gestiti da chi li riceve in completa autonomia quindi in qualità di Titolare. Per semplificare la diffusione delle informative, soprattutto considerando che i lavoratori coinvolti potrebbe non avere facilità ad accedere alle varie informative eventualmente presenti nei siti delle varie società, si è previsto di far fornire direttamente dal datore di lavoro ai propri lavoratori i cui dati potrebbero essere consegnati ad altre società, oltre alla normale informativa aziendale, una informativa standard specifica per questi dati.

Se il titolare che acquisisce i dati non si riconosce nell'informativa standard (ed esempio perché intende trasmettere i dati in paesi terzi) dovrà preoccuparsi di fornire direttamente l'informativa a tutti gli interessati. Negli altri casi sarà sufficiente che trasmetta i dati di contatto del Titolare.

Il Datore di Lavoro deve essere, in ogni momento, in grado di fornire al proprio lavoratore i dati di tutti i Titolare che sono in possesso dei suoi dati.



Ogni Titolare della filiera delle costruzioni dovrà consegnare a tutti i propri lavoratori l'informativa aziendale relativa ai trattamenti svolti dall'azienda sui dati personali del lavoratore (per gli stipendi, la formazione, ecc.).

Ai lavoratori che possono operare nei Cantieri verrà consegnata anche la "Informativa per i Lavoratori di altre imprese impegnati nei Cantieri" relativa al trattamento che altri Titolari potranno fare sui dati personali del lavoratore.

Chiunque riceve i dati dei Lavoratori di altre imprese (Appaltatore, Committente, ecc.) li dovrà trattare conformemente a quanto previsto dall'informativa "standard" o dovrà preoccuparsi di fornire una propria informativa alternativa.

Informativa ai Clienti (Inf_01)

Nel caso in cui il Cliente sia una persona fisica o una Società senza personale o che comunque possa fornire unicamente i dati personali della persona fisica che firma l'informativa è stata predisposta una informativa diretta all'interessato.

Lo scambio di informazioni di natura commerciale si ritiene legittimato dall'interesse del titolare e si assicura agli interessati di potersi opporre senza alcuna formalità al trattamento.

Informativa alle Società Clienti (Inf_04a)

L'informativa, al fine di limitare l'uso di dati personali a quanto strettamente necessario (Art. 5 1/c del RGPD), richiede alle Società con le quali si entra in contatto di fornire, per quanto possibile, unicamente dati aziendali.

Nei rapporti fra società è comunque possibile che sia necessario fornire alcuni dati personali. L'informativa alla Società Cliente ha lo scopo di fornire tutte le informazioni necessarie alle persone fisiche [interessati] i cui dati personali vengono forniti dalla Società Cliente alla Società.

Sarà cura della Società Cliente informare gli interessati che i loro dati potranno essere trattati dalla Società e fornire loro le informazioni essenziali della informativa (diritti, punti di contatto, ecc.)

È previsto di trattare unicamente dati COMUNI.

Anche in questo caso lo scambio di informazioni di natura commerciale si ritiene legittimato dall'interesse del titolare e si assicura alla Società Cliente ed agli interessati di potersi opporre senza alcuna formalità al trattamento.

Informativa per i Committenti (Inf_04b)

Qualora il Cliente sia un Committente i dati di contatto del Titolare che acquisisce i dati dei lavoratori che entrano nel Cantiere potranno venire utilizzati per essere comunicati ai lavoratori che ne facciano richiesta.

Si segnala inoltre che i lavoratori hanno ricevuto la "Informativa per i Lavoratori di altre imprese impegnate nei Cantieri Edili", qualora il Committente non desideri utilizzarla dovrà provvedere a fornire direttamente l'informativa agli interessati.

Informativa ai Fornitori (Inf_05)

In generale valgono le stesse considerazioni fatte per i Clienti ma in questo caso la possibilità di riattivare relazioni commerciali rientra nella gestione di un normale ambito precontrattuale (richiesta di offerte).

Informativa alle Società Fornitrici (Inf_05a)

Valgono le stesse considerazioni fatte per le Società Clienti ed anche in questo caso la possibilità di riattivare relazioni commerciali rientra nella gestione di un normale ambito precontrattuale (richiesta di offerte).

Informativa ai Subappaltatori o Fornitori di Servizi (Inf_05b)

Nel caso la Società Fornitrice sia un Subappaltatore viene richiesto di consegnare la "Informativa per i Lavoratori di altre imprese impegnate nei Cantieri Edili" a tutti i lavoratori dei quali potrà fornirci i dati personali per provvedere alla gestione della sicurezza nel Cantiere D.Lgs. n. 81/2008 e per permettere la corretta gestione dalla responsabilità solidale ex art. 29 del D.Lgs. n. 276/2003.

Il Subappaltatore dovrà organizzarsi per fornire ai propri dipendenti l'elenco dei Titolari che sono entrati in possesso dei loro dati per ogni Cantiere.

Informativa per i Currucula (Inf_06)

"Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto." (Art. 111-bis D.Lgs. 196/03).

Informativa per le Mail (Inf_07)

L'informativa contiene tutte le informazioni opportune. Visto il rischio di consumo di carta nel caso di stampa della mail viene suggerito di inserire l'informativa completa sul sito aziendale (quando presente) e richiamarla semplicemente sotto ogni mail.

Informativa per il Sito aziendale (Inf_08)

L'informativa presuppone che il Sito dell'Azienda utilizzi unicamente "cookie tecnici" o equiparabili (es, "cookie analytics" che precludono la possibilità di individuazione dell'interessato) per i quali non è necessario il consenso. Il titolare del trattamento sarà, quindi, assoggettato al solo obbligo di fornire specifica informativa che dovrà indicare i cookie tecnici utilizzati [come indicato nelle Linee Guida del 10 Giugno 2021]. In questi casi l'informativa può essere collocata nella home page del sito.

Misure da adottare qualora nel sito dell'azienda siano presenti altri tipi di cookie.

Dovrà essere cura del Titolare assicurare che il sito permetta, a chi naviga nel sito, di bloccarli fornendo adeguata informativa e richiedendo, dove necessario, il consenso (che è l'unico elemento che rende legittimo il trattamento per i cookie analitici di terze parti non anonimizzati o per i cookie di profilazione) tramite un apposito banner direttamente sul sito.

Si ricorda che il consenso non può essere raccolto tramite il semplice "scroll down" del cursore ma deve essere espresso dall'interessato attraverso un atto positivo inequivocabile.

Il titolare dovrà garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non eccedano il minimo necessario per il conseguimento delle finalità perseguite, in modo che l'utilizzo di informazioni per l'accesso ad un sito sia inizialmente limitato al minimo indispensabile per consentirne la fruizione e che sia rimesso interamente all'interessato un effettivo, concreto potere di scelta in ordine alla possibilità di consentire o meno un utilizzo eventualmente più ampio dei suoi dati.

Designazioni

Designazione di Referenti: Documento Base (Nom_0)

Il Titolare può designare dei Referenti che assicurino il rispetto delle disposizioni del Titolare.

A tal fine è stata predisposta una Designazione di Referenti che contiene le seguenti sezioni:

- l'ambito di competenza del Referente;
- i controlli che il Referente dovrà attuare;
- i limiti alla comunicazione e diffusione dei dati personali;
- le Misure di sicurezza che dovrà assicurare;
- la gestione di incidenti e violazioni;
- le Verifiche sulla gestione dei dati personali.

Varianti

Designazione Referente per il Sistema Informativo (Nom_1)

All'interno di ogni azienda, quando possibile, è opportuno designare un RSI che sarà un primo riferimento per tutti gli autorizzati e che si interfaccerà e coordinerà le attività dei consulenti IT.

Designazione Referente Tecnico per il Sistema Informatico (Nom_1a)

In alcuni casi l'azienda può individuare un RTSI che affiancherà l'RSI per le problematiche tecniche. In genere l'RTSI sarà una società esterna che opererà come Responsabile con la quale andrà stipulato un accordo per il trattamento dei dati (vedi 5.3).

Designazione Referente Privacy (Nom_2)

Il termine Responsabile nel GDRP è riservato ai soggetti che operano in outsourcing. All'interno dell'azienda il Titolare può designare dei Referenti per le varie Aree/Uffici (es. Amministrazione, Gestione Personale, ecc.) che coordineranno l'attività degli autorizzati a trattare i dati personali a Loro sottoposti.

Alcuni Referenti potranno essere responsabili di specifiche aree di memorizzazione (Cartelle di Windows, Cartelle sul Cloud, ecc.) dei dati aziendali e dovranno controllare la cancellazione dei dati personali contenuti (in funzione del periodo di conservazione stabilito) e definire gli autorizzati che hanno necessità di accedere ai dati contenuti e quelli eventualmente da rimuovere.

Qualora ai Referenti sia affidata la responsabilità di caselle di posta condivise (info@DOMINIO, amministrazione@DOMINIO, ecc.) dovrà definire le modalità di utilizzo (criteri per la lettura e lo smistamento, criteri per l'eliminazione dei messaggi, ecc.), controllare la cancellazione dei dati personali contenuti (in funzione del periodo di conservazione stabilito) e definire gli autorizzati che hanno necessità di accedere ai dati contenuti e quelli eventualmente da rimuovere.

Designazione degli Autorizzati Base (Des_0)

L'Art. 32 del RGPD prevede che le persone autorizzate (in precedenza anche "incaricati") trattino i dati solo in base a specifiche istruzioni.

A tal fine è stata predisposta una Designazione che contiene le seguenti sezioni:

- Accesso e creazione banche dati.
- Comunicazione e diffusione.
- Misure di sicurezza.
- Verifiche sulla gestione dei dati personali.

Varianti

Designazione Autorizzato al trattamento (Des_1)

È la designazione per tutti gli autorizzati a trattare i dati personali.

Designazione Responsabile del Servizio Prevenzione e Protezione (Des_2)

Il ruolo di RSPP, quando previsto, non richiede trattamenti specifici sui dati ma, potendo avere nozione di dati anche "particolari" è opportuno prevedere una designazione nella quale vengano ribaditi gli aspetti legati alla sicurezza dei dati personali. Qualora l'RSPP svolga anche altre attività per la società (quali pianificazione della Formazione, redazione del DVR o dei POS, ecc.) è opportuno stipulare un accordo in qualità di Responsabile Esterno di Trattamenti svolti per conto del Titolare.

Designazione Membro Organismo di Vigilanza (Des_3)

Con riferimento al GRPD 679/2016 relativo al trattamento dei dati personali, i componenti dell'OdV e l'organismo nel suo insieme agiscono in qualità di soggetto autorizzato al trattamento dei dati, nel rispetto delle istruzioni che debbono essere impartite dal Titolare del Trattamento per garantire che il trattamento stesso avvenga in conformità ai principi stabiliti dall'art. 5 del Regolamento.

È stata quindi prevista una specifica designazione relativa allo svolgimento delle attività necessarie all'espletamento dei compiti di vigilanza e controllo attribuiti all'Organismo di Vigilanza ai sensi del D.Lgs. 231/2001, nonché all'adempimento degli obblighi informativi previsti sia in capo al medesimo OdV che alle funzioni aziendali/organi di vertice rispetto alle criticità rilevate in merito all'organizzazione della Società e al funzionamento e all'aggiornamento del Modello di organizzazione, gestione e controllo.

NOTA: la designazione quale autorizzato proposta ha ad oggetto solo il ruolo, ai fini privacy, che l'OdV assume con riferimento ai flussi di informazioni rilevanti ai sensi dell'art. 6, commi 1 e 2 del d.lgs. n. 231/2001. Qualora ai membri dell'OdV vengano assegnati altri ruoli (quali, ad esempio la gestione delle segnalazioni effettuate nell'ambito della normativa di whistleblowing) andrà individuata la corretta qualificazione soggettiva ai fini privacy.

Nello svolgimento delle proprie funzioni, i componenti dell'OdV possono venire a conoscenza di dati comuni anagrafici e relativi alle attività lavorative svolte ma anche dati di natura particolare, secondo la definizione contenuta nell'art. 9 del RGPD, (es. Idoneità con prescrizioni, permessi particolari, richieste relative a familiari), nonché dati relativi a condanne penali (quando la loro conoscenza è possibile, ai sensi della legge - art. 10, RGPD). I dati potranno essere, comunque, trattati unicamente se ricorrono le condizioni previste dal Regolamento.

Vista la specificità dell'autorizzazione vanno previste particolari misure di sicurezza. In particolare, i dati in formato digitale potranno essere memorizzati sui server aziendali solo in cartelle dove hanno i diritti d'accesso solo i membri dell'OdV. Se un membro dell'OdV decide di memorizzare i dati su propri dispositivi questi devono essere adeguatamente protetti da password e, in caso di dispositivi mobili, crittografati. I dati in formato cartaceo dovranno essere sempre riposti in armadi le cui chiavi sono a disposizione unicamente dei membri dell'OdV e dovranno essere applicate le misure di sicurezza appropriate (controllati con la massima diligenza e attenzione durante tutto il periodo in cui vengono utilizzati; non dovranno essere lasciati incustoditi sulle scrivanie in caso di assenze prolungate e, al termine dell'attività espletata, deve essere riposto nel luogo sicuro).

Designazione Membro Collegio Sindacale (Des_4)

Qualora presenti i membri del Collegio Sindacale devono essere autorizzati al trattamento dei dati personali.

Accordi per il trattamento dei dati con i Responsabili

Documento Base (Resp)

I documenti proposti possono servire sia per definire con tutti i Responsabili con i quali già esiste un Contratto di servizi che però non contiene aspetti legati alla privacy o li contiene ma non secondo le disposizioni dell'Art. 28 del RGPD anche alla luce della pubblicazione delle Clausole contrattuali tipo sia per definire i nuovi contratti rendendo chiari gli aspetti legati alla privacy.

I documenti devono necessariamente essere personalizzati in funzione del trattamento assegnato al Responsabile.

Clausole contrattuali tipo (Resp_1_CCT_Senza_Allegati)

Si prevede di utilizzare integralmente ed unicamente le "Clausole contrattuali tipo" proposte dalla Commissione Europea con riferimento al regolamento (UE) 2016/679, scegliendo, per il ricorso a sub-responsabili, l'opzione 2 (autorizzazione scritta generale) e rimandando all'Allegato III per la specifica del periodo di anticipo per la comunicazione al titolare del trattamento di eventuali modifiche riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento.

Allegati base (Resp_2_CCT_Allegati_Base)

Per gli Allegati è stato predisposto un documento di base nel quale gli Allegati I e II sono riportati inalterati mentre nell'Allegato III sono state suddivise le misure in base alla tipologia (anche sulla base degli esempi riportati nella nota esplicativa).

Viene indicato (in verde) per quali casistiche di trattamento sono pensate le misure proposte (es. trattamento di dati in formato cartaceo, trattamento svolto presso la sede del titolare, ecc.). Ovviamente, questa informazione andrà eliminata dal documento finale.

Alcune misure sono ritenute fondamentali mentre altre (evidenziate in arancione) possono inserite in base alla valutazione del titolare; alcune misure (evidenziate in rosso) possono risultare particolarmente stringenti per i responsabili e quindi verranno inserite dal titolare solo dopo una attenta valutazione del livello di sicurezza ritenuto adeguato, tenendo conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

Per l'Allegato II sono proposte varie ipotesi per i vari Trattamenti come illustrato di seguito.

Check List (Resp_3_Check_List)

Le Clausole contrattuali tipo soddisfano i requisiti dei paragrafi 3 e 4 dell'Art. 28 del RGPD. Al fine di semplificare gli obblighi per il titolare presenti nel paragrafo 1 relativi all'analisi delle garanzie sulle misure tecniche e organizzative messe in atto dal Responsabile è stata predisposta una "Check-list sull'adeguatezza del Responsabile" che, ove necessario, il Responsabile dovrà compilare e che dovrà essere valutata adeguata dal Titolare prima della firma dell'accordo stesso. Viene fornito anche un esempio di "Rapporto periodico del Responsabile del trattamento dei dati" che permette al Titolare di verificare il costante rispetto delle garanzie.

La clausola 7.7 a) prevede l'obbligo del responsabile di informare il titolare in caso di modifiche riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento. Per facilitare la comunicazione è presente la scheda "Elenco degli altri Responsabili".

Il Titolare dovrà valutare in quali casi trasmettere questi documenti ai Responsabili.

Varianti

Amministrazione del personale (Trattamento_1)

I Responsabili che gestiscono esternamente i dati relativi all'amministrazione del personale possono trattare dati di categorie particolari, quindi, è particolarmente importante la valutazione dell'adeguatezza nel trattamento dei dati.

Gestione Contabile (Trattamento_2)

I Responsabili che gestiscono esternamente i dati relativi alla gestione contabile potrebbero venire a conoscenza di dati personali.

Manutenzione dei sistemi informatici (Trattamento_3)

Le società che effettuano manutenzione dei Sistemi Informatici non trattano i dati presso la propria sede ma operano direttamente sui sistemi informatici del Titolare. Possono quindi venire a conoscenza, anche involontariamente, di alcuni dati personali di titolarità del Titolare.

In generale, nel compiere i servizi previsti dal Contratto possono compromettere, anche per un insieme notevole di dati, la disponibilità, la riservatezza e l'integrità.

Manutenzione dei pacchetti software gestionali (Trattamento_4)

Le società che effettuano manutenzione dei pacchetti software gestionali possono, oltre che operare presso la sede del cliente (anche da remoto), effettuare copie dei dati del Titolare, ad esempio per verificare specifiche anomalie riscontrate, che possono essere trattate presso la sede del Responsabile.

Distributore di software SAAS (Trattamento_5)

Le società che utilizzano strumenti software offerti dai produttori che sviluppano e gestiscono applicazioni web, mettendole a disposizione dei propri clienti via Internet (cloud computing) devono definire un rapporto con i produttori che assicuri le misure di sicurezza.

Amministratori di sistema (Trattamento_6a, Trattamento_6b)

Sono previsti due documenti: uno qualora il contratto sia stato stipulato con il singolo Amministratore di Sistema ed uno nel caso in cui il contratto sia con la società che fornisce gli Amministratori di Sistema.

Responsabile del Servizio Prevenzione e Protezione (Resp_7)

Il ruolo di RSPP non richiede trattamenti specifici sui dati. Qualora l'RSPP svolga anche altre attività per la società (quali pianificazione della Formazione, redazione del DVR o dei POS, ecc.) è opportuno stipulare un accordo in qualità di Responsabile di Trattamenti svolti per conto del Titolare.

In questi casi l'RSPP può trattare dati, anche di categorie particolari, sulla propria strumentazione elettronica anche presso la propria sede.

Registro semplificato per le imprese di Costruzione

Ogni Trattamento è caratterizzato da:

- un Codice (che verrà utilizzato anche per l'ordine di presentazione dei vari trattamenti);
- l'Area di riferimento (Gestione del Personale, Gestione Clienti, Gestione Fornitori, Dati Amministrativi, ecc.);
- la descrizione del trattamento;
- finalità del trattamento;
- le categorie di interessati;
- una valutazione sulla significatività del trattamento;
- categorie di dati personali trattati;
- punti del paragrafo 1 dell'Art. 6 che rendono lecito il trattamento;
- categorie particolari di dati personali trattati (ex "sensibili");
- punti del paragrafo 2 dell'Art. 9 che rendono lecito il trattamento per categorie particolari di dati;
- formato dei dati trattati (Cartaceo e/o Digitale);
- autorizzati al trattamento;
- eventuali Responsabili Esterni che partecipano al trattamento;
- destinatari esterni;
- eventuale trasferimento dati verso paesi terzi o organizzazioni internazionali;
- termini ultimi di cancellazione previsti;
- misure di sicurezza tecniche e organizzative;
- documento utilizzato per fornire le informazioni sul trattamento;
- modalità utilizzate per raccogliere il consenso quando necessario.

DATI INTERNI

Possono essere definiti anche dati non richiesti per la compilazione del Registro dei Trattamenti semplificato ma che possono essere utili per la corretta gestione quali, ad esempio:

- Referente Privacy (colui che sovrintende al trattamento in oggetto) - Ufficio.
- Note interne.
- Data di Inizio del trattamento ed eventuale data di conclusione.
- Data di creazione e dell'ultimo Aggiornamento o verifica di adeguatezza.
- Tempo massimo di interruzione (MTPD: *Maximum tolerable period of disruption*), ossia il tempo massimo per cui il processo può non essere operativo
- Massima perdita di dati (MTDL: *Maximum Tollerance Data Loss*), intesa come tempo trascorso dall'ultimo salvataggio e, quindi, corrispondente ai dati da ricostruire una volta persi.

ELEMENTI DEL TEST DI BILANCIAMENTO PER TRATTAMENTI BASATI SUL LEGITTIMO INTERESSE (Qualora la base giuridica per un trattamento sia il Legittimo interesse del Titolare)

- Valutazione dell'interesse legittimo da parte del Titolare.
  Nota: Dovrà inoltre essere abbastanza specifico e articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del Titolare rispetto agli interessi e ai diritti fondamentali dell'interessato. Dovrà altresì rappresentare un interesse concreto ed effettivo, ossia non essere teorico. Andrà valutato se esistono altri mezzi meno invasivi per conseguire lo scopo specifico.
- Impatto sugli interessi ed i diritti degli interessati.
  Nota: Tenere conto della natura dei dati, lo status dell'interessato (es. minore, lavoratore dipendente), la modalità del trattamento (su vasta scala, comunicazione ad un ampio numero di persone, ecc.). Individuare gli interessi ed i diritti dell'interessato su cui potrebbe incidere il trattamento. Considerare le ragionevoli aspettative degli interessati.
- Bilanciamento provvisorio (in assenza di garanzie supplementari).

- Eventuali garanzie supplementari rispetto agli obblighi previsti dal RGPD (da applicare qualora il bilanciamento provvisorio sia dubbio e non è chiaro se prevale il legittimo interesse del Titolare).

  Nota: Minimizzazione dei dati raccolti e loro immediata cancellazione dopo l'utilizzo. Misure tecniche ed organizzative volte a garantire che i dati non possano essere utilizzati per intraprendere azioni riguardo alle persone. Diritto incondizionato di opposizione. Diritto di accesso ai propri dati.

Esempio di Registro dei trattamenti

Cod.	Area	Descrizione	Finalità	Categorie Interessati	Signifi-catività	Categorie dati Personali	Liceità (art. 6 par. 1)	Categorie Particolari dei dati Personali	Liceità cat. Particolari (art. 9 par 2)	Formato	Autorizzati	Responsabili Esterni	Destinatari esterni	Trasferimento dati verso paesi terzi o organizzazioni internazionali	Termini ultimi di cancellazione previsti	Misure di sicurezza tecniche e organizzative	Documento utilizzato per fornire le informazioni sul trattamento	Modalità richiesta consenso (solo se necessario)
P01	Gestione Personale	Assunzione, Rapporti Interinali e Contratti di collaborazione	Raccolta e Archiviazione dati del lavoratore per stipula del contratto.	Dipendenti / Collaboratori continuativi	Media	Dati anagrafici, recapiti, titoli di studio, qualifiche professionali, precedenti esperienze lavorative.	c.	Dati sulla salute e iscrizione sindacale.	b.	Digitale e Cartaceo	Ufficio Personale	Agenzie interinali.	Inail, INPS e altri enti di previdenza sociale.	Nessuno	5 anni dalla conclusione del rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti. Informativa Collaboratori.	
P02	Gestione Personale	Buste Paga e documentazione fiscale del lavoratore	Elaborazione e buste paga e documenti fiscali del lavoratore.	Dipendenti	Bassa	Dati anagrafici e dati sulla situazione economica dei familiari in caso di richiesta di detrazioni per carichi di famiglia o assegni per nucleo familiare.	b.	Dati sulla salute ricavabili da assenze	b.	Digitale e Cartaceo	Ufficio Personale	Consulente del lavoro o Società elaborazione paghe.	Inail, INPS e altri enti di previdenza sociale.	Nessuno	5 anni dalla conclusione del rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti.	
P03	Gestione Personale	Definizione mansioni	Descrizione delle attività del lavoratore.	Dipendenti / Collaboratori continuativi	Media	Dati anagrafici, titoli di studio, qualifiche professionali, precedenti esperienze lavorative.	b.	Nessuno		Digitale e Cartaceo	Ufficio Qualità			Nessuno	Conservazione per difesa aziendale.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti. Informativa Collaboratori.	
P04	Gestione Personale	Sanzioni Disciplinari	Definizione, Gestione, Comunicazione e Archiviazione delle Sanzioni Disciplinari.	Dipendenti	Alta	Dati anagrafici, rilievi, sanzioni.	b.	Nessuno		Digitale e Cartaceo	Direzione		Legale, Sindacato.	Nessuno	5 anni dalla conclusione del rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti.	

Cod.	Area	Descrizione	Finalità	Categorie Interessati	Signifi-catività	Categorie dati Personali	Liceità (art. 6 par. 1)	Categorie Particolari dei dati Personali	Liceità cat. Particolari (art. 9 par 2)	Formato	Autorizzati	Responsabili Esterni	Destinatari esterni	Trasferimento dati verso paesi terzi o organizzazioni internazionali	Termini ultimi di cancellazione previsti	Misure di sicurezza tecniche e organizzative	Documento utilizzato per fornire le informazioni sul trattamento	Modalità richiesta consenso (solo se necessario)
P05	Gestione Personale	Visite Mediche	Pianificazione e Archiviazione delle Visite per idoneità alla mansione e relativi aggiornamenti.	Dipendenti / Collaboratori continuativi	Alta	Dati anagrafici, mansioni svolte. Eventuali prescrizioni su limitazioni.	c.	Dati relativi a rilevare l'idoneità lavorativa.	h.	Digitale e Cartaceo	Ufficio Personale			Nessuno	Conservazione per difesa aziendale.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti. Informativa Collaboratori.	
P06	Gestione Personale	Formazione	Pianificazione, Svolgimento e Archiviazione della formazione dei lavoratori.	Dipendenti / Collaboratori continuativi	Media	Dati anagrafici, mansioni svolte, formazioni effettuata.	c (per la formazione obbligatoria), f.(per quella aziendale).	Nessuno		Digitale e Cartaceo	Ufficio Personale			Nessuno	Conservazione per difesa aziendale.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti. Informativa Collaboratori.	
P07	Gestione Personale	Dimissione	Gestione della conclusione del contratto.	Dipendenti	Bassa	Dati anagrafici. Condizioni contrattuali.	b.	Nessuno		Digitale e Cartaceo	Ufficio Personale	Consulente del lavoro o Società elaborazione paghe.	Legale, Sindacato.	Nessuno	5 anni dalla conclusione del rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti.	
P08	Gestione Personale	Infortuni	Raccolta, Gestione, Comunicazione (agli Enti e alle Assicurazioni), Elaborazione statistiche e Archiviazione degli infortuni.	Dipendenti	Alta	Dati anagrafici, mansioni svolte, conseguenze dell'incidente.	c.	Dati sulla salute.	h.	Digitale e Cartaceo	Ufficio Sicurezza		Medico Competente, Legale, Sindacato.	Nessuno	Conservazione per difesa aziendale.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti.	
P09	Gestione Personale	Richieste dirette del personale (Permessi, ferie, 104 ecc.)	Gestione dei permessi del personale.	Dipendenti / Collaboratori continuativi	Media	Dati anagrafici anche di familiari. Dati relativi alla richiesta che potrebbero rilevare informazioni "sensibili" del dipendente e dei familiari.	b.	Dati potenzialmente in grado di rilevare le opinioni politiche, il credo religioso e lo stato di salute (anche dei familiari).	b.	Digitale e Cartaceo	Ufficio Personale		Inail, INPS e altri enti di previdenza sociale.	Nessuno	5 anni dalla conclusione del rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Dipendenti. Informativa Collaboratori.	

Cod.	Area	Descrizione	Finalità	Categorie Interessati	Signifi-catività	Categorie dati Personali	Liceità (art. 6 par. 1)	Categorie Particolari dei dati Personali	Liceità cat. Particolari (art. 9 par 2)	Formato	Autorizzati	Responsabili Esterni	Destinatari esterni	Trasferimento dati verso paesi terzi o organizzazioni internazionali	Termini ultimi di cancellazione previsti	Misure di sicurezza tecniche e organizzative	Documento utilizzato per fornire le informazioni sul trattamento	Modalità richiesta consenso (solo se necessario)
P10	Gestione Personale	Curricula	Raccolta e utilizzo dei CV per eventuali assunzioni/collaborazioni	Potenziali Dipendenti / Collaboratori	Bassa	Dati anagrafici, recapiti, titoli di studio, qualifiche professionali, precedenti esperienze lavorative. Interessi ed aspettative.	b.	Nessuno		Digitale e Cartaceo	Ufficio Qualità		Altre Imprese coinvolte in ATI o Consorzi (solo se espressamente autorizzati).	Nessuno	5 anni dalla ricezione.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Curricula sul Sito.	
P11	Gestione Personale	Segnalazioni	Conformità al D.Lgs. 24/ 2023	Dipendenti / Collaboratori (segnalante, segnalato e soggetti coinvolti)	Alta	Dati identificativi del Segnalante e dati sul segnalato o altri soggetti coinvolti	c.	Potenzialmente presenti all'interno delle segnalazioni	b.	Digitale e Cartaceo	Autorizzati al trattamento delle segnalazioni.	Gestore della piattaforma per le segnalazioni. Gestore esterno dei canali.	Nessuno	Nessuno	5 anni dalla chiusura.	Sicurezza della piattaforma. Segregazione eventuali documenti cartacei.	Informativa Dipendenti. Informativa Collaboratori. Inform\ativa per il segnalante sul sito.	
TC1	Gestione Clienti (Persone fisiche)	Gestione Anagrafica Clienti	Raccolta, Utilizzo per rapporti commerciali ed Archiviazione dati del Cliente.	Clienti persone fisiche.	Molto Bassa	Dati anagrafici e di contatto.	b.	Nessuno		Digitale e Cartaceo	Ufficio Amministrativo			Nessuno	10 anni dall'ultimo rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Clienti (persone fisiche) sul Sito.	
TC2	Gestione Clienti (Persone fisiche)	Richieste "sensibili" Clienti	Esecuzione di lavori che possano rilevare lo stato di salute di persone fisiche.	Clienti persone fisiche e familiari.	Alta	Dati anagrafici e di contatto.	b.	Dati potenzialmente in grado di rilevare lo stato di salute del Cliente o di suoi familiari.	a.	Digitale e Cartaceo	Ufficio Tecnico e Cantiere			Nessuno	10 anni dalla consegna dei lavori.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Clienti (persone fisiche) sul Sito.	
TF1	Gestione Fornitori	Gestione Anagrafica Fornitori (Persone fisiche)	Raccolta, Utilizzo per rapporti commerciali ed Archiviazione dati del Cliente.	Fornitori persone fisiche.	Bassa	Dati anagrafici e di contatto.	b.	Nessuno		Digitale e Cartaceo	Ufficio Amministrativo			Nessuno	10 anni dall'ultimo rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Fornitori (persone fisiche) sul Sito.	
TF2	Gestione Fornitori	Controllo Regolarità subappalti	Controllo Regolarità subappalti relativamente al pagamento delle	Dipendenti dei subappaltatori.	Alta	Dati anagrafici, dati idoneità, dati sul pagamento	b.			Digitale e Cartaceo	Ufficio Tecnico e Cantiere.			Nessuno	3 anni dalla chiusura del cantiere.	Sicurezza Sistema Informatico. Sicurezza nella		

Cod.	Area	Descrizione	Finalità	Categorie Interessati	Signifi-catività	Categorie dati Personali	Liceità (art. 6 par. 1)	Categorie Particolari dei dati Personali	Liceità cat. Particolari (art. 9 par 2)	Formato	Autorizzati	Responsabili Esterni	Destinatari esterni	Trasferimento dati verso paesi terzi o organizzazioni internazionali	Termini ultimi di cancellazione previsti	Misure di sicurezza tecniche e organizzative	Documento utilizzato per fornire le informazioni sul trattamento	Modalità richiesta consenso (solo se necessario)
			retribuzioni ed eventuali idoneità con prescrizioni.			delle retribuzioni.					Ufficio amministrativo.					gestione dei documenti cartacei.		
TF3	Gestione Fornitori	Sanzioni ai Fornitori (con dati persone fisiche)	Applicazione delle sanzioni previste contrattualmente.	Fornitori persone fisiche.	Media	Dati anagrafici, dati di contatto. Non Conformità rilevate.	b.	Nessuno		Digitale e Cartaceo	Ufficio Qualità			Nessuno	5 anni dalla conclusione del rapporto.	Sicurezza Sistema Informatico. Sicurezza nella gestione dei documenti cartacei.	Informativa Fornitori (persone fisiche) sul Sito.	

Policy e Procedure

Policy per gli Autorizzati (Policy)

È un esempio di Policy e Prescrizioni per gli autorizzati al trattamento dei dati.

Il documento contiene molte indicazioni, non solo strettamente legate alla gestione dei dati personali, per chi, all'interno dell'azienda, tratta le informazioni.

Questo documento dovrà essere personalizzato dal titolare, eventualmente con il supporto dei consulenti informatici che seguono l'azienda.

Il documento dovrebbe essere consegnato ad ogni autorizzato anche come parte dell'attività formativa.

Procedure

Procedura per la gestione delle violazioni (Proc_1)

È un esempio di procedura utilizzabile per la gestione delle violazioni.

Il titolare può personalizzare il documento per l'analisi del proprio sistema informativo e per essere pronto a reagire tempestivamente in caso di violazione riguardante dati personali.

Nella procedura si prevede che la segnalazione venga fatta direttamente al titolare, per aziende strutturate è possibile prevedere una scalabilità (es. che rileva la violazione comunica al suo diretto superiore che effettua una prima valutazione prima di informare il Titolare).

La procedura prevede che i Responsabili abbiano l'obbligo di comunicare al Titolare eventuali violazioni.

Procedura per l'esercizio dei diritti degli Interessati (Proc_2)

È un esempio di procedura utilizzabile per la gestione delle attività da compiere a seguito della richiesta, da parte di un interessato, di esercitare uno dei suoi diritti.

Procedura per l'ufficio del Personale (Proc_3)

Visto il trattamento di dati, anche appartenenti a categorie particolari, si è ritenuto opportuno predisporre una procedura per gli autorizzati che operano nell'ufficio del personale.

La Procedura tiene conto delle "*Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (Deliberazione n. 53 del 23 novembre 2006)*" emesse dal Garante Italiano e del "*Parere 2/2017 sul trattamento dei dati sul luogo di lavoro*" del Gruppo di Lavoro europeo per la protezione dei dati.

Trattamenti specifici

Documento Base (DPIA_Base)

Come previsto dall'Art. 35 del RGPD "Quando un tipo di trattamento … può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto [*anche DPIA*] dei trattamenti previsti sulla protezione dei dati personali".

È stata predisposta una bozza di DPIA che contiene gli elementi da analizzare per produrre le valutazioni d'impatto.

Anche se la pubblicazione della valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati i Titolari potranno valutare di renderla pubblica per contribuire a stimolare la fiducia nei confronti del trattamento e per dimostrare la responsabilizzazione e la trasparenza del Titolare.

In ogni caso non si ritiene opportuno pubblicare tutte le misure di sicurezza adottate per non fornire informazioni ad eventuali malintenzionati che potrebbero sfruttarle per un attacco mirato.

Sono stati analizzati alcuni trattamenti ed in alcuni casi sono state predisposte anche le relative procedure.

Videosorveglianza

Procedura per l'utilizzo di dispositivi video (Procedura_Videosorveglianza)

La procedura fornisce indicazioni sulla gestione della Videosorveglianza tenendo conto delle Linee Guida emesse nel 2019 dal "European Data Protection Board" e dalle indicazioni fornite dal Garante italiano (tra cui faq pubblicate sul suo sito e il Provvedimento 8 aprile 2010 per le parti ancora applicabili).

Valutazione d'impatto per l'uso di dispositivi video (DPIA_Videosorveglianza)

Contiene gli elementi essenziali per una valutazione d'impatto che dovranno essere personalizzate per lo specifico trattamento.

Cartello da esporre nell'area ripresa (Cartello_Videosorveglianza)

Viene presentato un esempio di cartello da esporre fuori dall'area ripresa per permettere all'interessato di avere le informazioni di primo livello e, attraverso un QR-Code, accedere all'informativa completa.

Informativa completa per le riprese video (Informativa_Videosorveglianza)

Le informazioni di primo livello presenti nei cartelli che devono essere visibili prima dell'ingresso nell'area sottoposta a riprese video non contengono tutte le informazioni necessarie che sono riportate nell'informativa completa alla quale l'interessato potrà accedere facendone richiesta o direttamente tramite QR-Code.

Geolocalizzazione

Procedura per le applicazioni relative alla mobilità (Procedura_Geolocalizzazione)

La procedura fornisce indicazioni sulla Geolocalizzazione tenendo conto delle Linee Guida emesse nel 2020 dal "European Data Protection Board".

Valutazione d’impatto per l’uso di dispositivi per la geolocalizzazione (DPIA_Geolocalizzazione)

Contiene gli elementi essenziali per una valutazione d’impatto che dovranno essere personalizzate per lo specifico trattamento.

Segnalazioni (whistleblowing)

Valutazione d’impatto per la gestione delle segnalazioni (DPIA_Segnalazioni)

Contiene gli elementi essenziali per una valutazione d’impatto che dovranno essere personalizzate per lo specifico trattamento.

3 APPENDICI

A. APPENDICE: Linee Guida sulla Trasparenza

Riferimenti

Articolo 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) 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.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) 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.

3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.

5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

Linee Guida sulla trasparenza relative al trattamento dei dati personali

Il Gruppo di lavoro consultivo dell'UE per la protezione dei dati personali e della vita privata (poi divenuto Gruppo di Lavoro Articolo 29 (WP29) e successivamente chiamato Comitato europeo per la protezione dei dati) ha predisposto delle Linee Guida sulla trasparenza relative al trattamento dei dati personali ed in particolare per:

- la fornitura agli interessati d'informazioni relative al trattamento corretto;
- le modalità con le quali il titolare del trattamento comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento;
- le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono.

Come tutte quelle emanate dal Gruppo, anche queste linee guida sono da intendersi come applicabili in generale ai titolari del trattamento, a prescindere dalle specifiche a livello settoriale o normativo tipiche per l'uno o l'altro di essi e mirano a consentire ai titolari del trattamento di comprendere come il Gruppo interpreti gli effetti pratici degli obblighi di trasparenza e a indicare l'approccio che, secondo il Gruppo, i titolari del trattamento dovrebbero adottare per essere trasparenti, ricomprendendo al contempo correttezza e responsabilizzazione nelle loro misure di trasparenza.

Di seguito vengono riportati gli elementi ritenuti essenziali per lo specifico settore delle costruzioni per supportare il Titolare del trattamento nel dimostrare che i dati sono trattati in modo trasparente nei confronti dell'interessato.

Linee Guida per la Trasparenza nel settore delle Costruzioni

Aspetti principali

Il significato della trasparenza e gli elementi ai sensi del RGPD

Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano concise, trasparenti, intelligibili e facilmente accessibili e che siano formulate con un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti. [6,7[5]]

L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica che il titolare del trattamento presenti le informazioni/comunicazioni in maniera efficace e succinta al fine di evitare un subissamento informativo. Tali informazioni dovrebbero essere

[5] I numeri fra parentesi quadra permettono il riferimento ai punti del documento originale.

differenziate nettamente da altre che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d'uso. Nell'ambiente online l'utilizzo di una dichiarazione/informativa sulla privacy stratificata consentirà all'interessato di consultarne immediatamente la specifica sezione desiderata, senza dover scorrere ampie porzioni di testo alla ricerca di un argomento in particolare. [8]

L'obbligo di fornire informazioni "intelligibili" implica che risultino comprensibili a tutti i destinatari. [9]

Le Associazioni proponenti hanno effettuato dei test di leggibilità sui documenti predisposti.

L'interessato deve essere sensibilizzato ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali e dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano.

Qualora un Titolare ritenga di effettuare un trattamento di dati per casi complessi, tecnici o inattesi (non previsti per una impresa di costruzioni standard) dovrà dichiarare, oltre alle informazioni previste nei documenti standard, in una sede distinta, in un linguaggio privo di ambiguità, quali saranno le principali conseguenze del trattamento, in altre parole, quale tipo di effetto sull'interessato, descritto in una dichiarazione/informativa sulla privacy, avrà concretamente il trattamento specifico. [10]

L'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili. [11]

Linguaggio semplice e chiaro

Le informazioni devono essere fornite nel modo più semplice possibile, evitando frasi e strutture linguistiche complesse. Le informazioni dovrebbero essere concrete e certe, non dovrebbero essere formulate in termini astratti o ambigui né lasciare spazio a interpretazioni multiple. In particolare, dovrebbero risultare chiare le finalità e la base giuridica del trattamento dei dati personali. [12]

Le informative e le comunicazioni proposte nelle presenti Linee Guida sono state scritte utilizzando le indicazioni fornite nel libro redatto dalla Commissione europea "Scrivere chiaro".

Si dovrebbe evitare l'uso di qualificatori linguistici come "può", "potrebbe", "alcuni", "spesso" e "possibile".

Se il titolare del trattamento sceglie di usare un linguaggio vago, conformemente al principio di responsabilizzazione dovrebbe essere in grado di dimostrare il motivo per cui tale linguaggio è inevitabile e il motivo per cui non compromette la correttezza del trattamento. [13]

I Documenti proposti nelle presenti Linee Guida cercano di strutturare i paragrafi e le frasi, utilizzando titolazioni, elenchi puntati e rientri per segnalare rapporti gerarchici. Per quanto possibile le informazioni fornite all'interessato non utilizzano linguaggio o terminologia eccessivamente legalistica, tecnica o specialistica.

Informazioni fornite a persone vulnerabili

I titolari del trattamento dei dati per imprese di costruzione standard non dovrebbero avere il problema di fornire informative per i minori ma, se consapevoli che le informative possono essere rivolte ad altri soggetti vulnerabili della società, tra cui persone con disabilità o persone che possono incontrare difficoltà ad accedere alle informazioni, dovrebbero tenere conto delle vulnerabilità di tali interessati nella valutazione del modo in cui assolvere gli obblighi di trasparenza nei loro confronti. [16]

Informazioni da fornire all'interessato

La qualità, l'accessibilità e la comprensibilità delle informazioni sono importanti così come i contenuti effettivi delle informazioni finalizzate alla trasparenza, che devono essere fornite agli interessati. [4, 24]

I documenti proposti tengono conto delle modalità della raccolta e del trattamento dei dati e sono stati valutati alla luce dell'esperienza degli interessati e, come già illustrato, sono stati sperimentati sui destinatari.

Tempistica

Le informazioni devono essere fornite nel momento in cui i dati personali sono ottenuti o, per i trattamenti già in corso prima dell'entrata in vigore del RGPD, devono essere portate attivamente all'attenzione dell'interessato. [3, 27]

Nel caso di dati personali ottenuti indirettamente, le tempistiche entro le quali le informazioni devono essere fornite all'interessato, sono ragionevolmente individuate-entro un mese. [27]

L'utilizzo della "Informativa per i Lavoratori di altre imprese impegnate nei Cantieri" garantisce l'informazione di tutti i Lavoratori sul trattamento dei loro dati ottenuti indirettamente.

Modifica delle informazioni

Le modifiche della dichiarazione/informativa sulla privacy dovrebbero essere sempre comunicate agli interessati (a meno di semplici correzioni di refusi o imprecisioni sintattiche o grammaticali).

L'eventuale modifica delle finalità del trattamento dovrà essere comunicata in modo tale da essere effettivamente recepita dai destinatari. [29]

Le modifiche relative all'identità del titolare del trattamento e del modo in cui gli interessati possono esercitare i diritti di cui godono in relazione al trattamento saranno sempre disponibili nel sito aziendale o nei documenti online [vedi avanti nella sezione Formato delle Informative].

Alla fine di ogni documento online vengono riportate le seguenti frasi:

Nell'elenco dei documenti online, accanto al nome, viene presentata la data dell'ultimo aggiornamento per permettere all'interessato di verificare la validità del documento consultato.

Gli aggiornamenti sono, in genere, orientati ad accrescere la tutela dei diritti degli interessati o per adeguarsi alle disposizioni delle autorità garanti; in caso di riduzione delle tutele sarà cura del Titolare informare di tali limitazioni tutti gli interessati che hanno fornito i propri dati antecedentemente alle modifiche.

Formato di fornitura delle informazioni

Nel RGPD è insita una tensione tra l'obbligo di fornire agli interessati le necessarie informazioni complete e quello di fornirle in una forma concisa, trasparente, intelligibile e facilmente accessibile [34].

A tal proposito è stata effettuata una analisi della natura, delle circostanze, della portata e del contesto del trattamento dei dati personali svolto dalle imprese di costruzione standard ed è stata valutata quale priorità assegnare alle informazioni da fornire agli interessati e quali livelli di dettaglio e metodi siano appropriati per trasmetterle.

Esercizio dei diritti degli interessati

La trasparenza impone al Titolare un triplice obbligo per quanto attiene ai diritti dell'interessato come previsto dal regolamento e cioè: [54]

- fornire informazioni agli interessati sui loro diritti;
- rispettare il principio di trasparenza nella comunicazione con gli interessati riguardo all'esercizio dei loro diritti;
- agevolare l'esercizio dei diritti degli interessati.

Le informazioni fornite devono rendere consapevoli gli interessati in modo che possano rivendicare i loro diritti e far ritenere i titolari del trattamento soggetti responsabilizzati in merito al trattamento dei dati personali che li riguardano.

I documenti proposti forniscono agli interessati le modalità per l'esercizio dei diritti appropriate al contesto e alla natura del rapporto e delle interazioni con il Titolare. [55]

Trasparenza nel caso di violazione dei dati

Sono stati predisposti i documenti per informare gli interessati in caso di violazione dei loro dati. [70]

Contenuti delle Informative

Informazioni da fornire all'interessato.	Considerazioni
Identità e dati di contatto del Titolare	Le informazioni dovrebbero consentire una facile identificazione del titolare del trattamento e preferibilmente varie forme di comunicazione con esso (ad es. numero di telefono, e-mail, indirizzo postale, ecc.).
Dati di contatto del responsabile della protezione dei dati.	NON APPLICABILE PER UNA IMPRESA DI COSTRUZIONE STANDARD. Si vedano le linee guida del Gruppo sui responsabili della protezione dei dati
Finalità e base giuridica del trattamento.	Oltre a definire le finalità del trattamento cui sono destinati i dati personali, deve essere specificata la relativa base giuridica (Art. 6). Nel caso delle categorie particolari di dati personali si dovrebbe specificare la disposizione applicabile (Art. 9).
Eventuali Legittimi interessi perseguiti dal Titolare o da un terzo.	Il Titolare dovrebbe fornire le informazioni tratte dal test di bilanciamento, che dev'essere svolto prima di raccogliere i dati personali degli interessati per poter addurre il legittimo interesse, o esplicitare loro la possibilità di ottenere, su richiesta, informazioni sul test di bilanciamento.
Categorie di dati personali non ottenuti dagli interessati.	Quando i dati personali non sono stati ottenuti presso l'interessato, il quale ignora pertanto quali categorie di dati personali il titolare del trattamento abbia ottenuto.
Destinatari	In genere i nomi dei destinatari, in maniera tale che gli interessati sappiano con precisione chi è in possesso dei dati personali che li riguardano. Se venissero fornite le categorie dei destinatari, le informazioni dovrebbero essere le più specifiche possibili e indicare il tipo (ad es. facendo riferimento alle attività svolte), l'ambito di attività, il settore, il comparto e la sede dei destinatari.
Informazioni sui trasferimenti a paesi terzi.	NON APPLICABILE PER UNA IMPRESA DI COSTRUZIONE STANDARD. Dovrebbe essere specificato l'articolo del regolamento che consente il trasferimento. Le informazioni fornite dovrebbero

Informazioni da fornire all'interessato.	Considerazioni
	essere il più pregnanti possibile per gli interessati compreso il nome dei paesi terzi.
Periodo di conservazione (o, se non disponibile, criteri per determinarlo).	Il periodo di conservazione (o i criteri per determinarlo) potrebbe essere dettato da obblighi di legge o dalle linee guida di settore, ma dovrebbe essere indicato in maniera tale da consentire all'interessato di stabilire quale sarà, in base alla sua specifica situazione, il periodo previsto per i dati. Non è sufficiente che il titolare del trattamento affermi in maniera generica che i dati personali saranno conservati finché sarà necessario per le finalità legittime del trattamento. Ove pertinente, dovrebbero essere fissati periodi di conservazione diversi per le diverse categorie di dati personali e/o finalità del trattamento, inclusi, se del caso, i periodi di archiviazione.
Diritti dell'interessato relativamente a: • accesso • rettifica • cancellazione • limitazione • opposizione • portabilità	Le informazioni dovrebbero essere specifiche per l'ipotesi di trattamento e comprendere una sintesi della natura dei diritti, del modo in cui l'interessato può attivarsi per esercitarli e delle loro eventuali limitazioni. In particolare, il diritto di opporsi al trattamento deve essere portato esplicitamente all'attenzione dell'interessato al più tardi al momento della prima comunicazione e deve essere presentato in forma chiara e separata da qualsiasi altra informazione.
Diritto di revocare il consenso in qualsiasi momento.	Le informazioni dovrebbero indicare il modo in cui il consenso può essere revocato, tenuto conto del fatto che esso dovrebbe poter essere revocato con la stessa facilità con cui è accordato.
Diritto di presentare un reclamo all'autorità di controllo.	Le informazioni dovrebbero spiegare che l'interessato ha diritto di presentare un reclamo all'autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente o lavora oppure nel luogo ove si è verificata la presunta violazione del regolamento.
Obbligatorietà di fornire informazioni e le conseguenze di un eventuale rifiuto.	È necessario indicare se esista o no un obbligo previsto per legge o per contratto di fornire le informazioni o se sia necessario stipulare un contratto o se sussista l'obbligo di comunicare le informazioni, e le possibili conseguenze dell'omissione. In un contesto di lavoro, ad esempio, potrebbe essere richiesto per contratto di fornire determinate informazioni al datore di lavoro presente o futuro. I moduli online dovrebbero indicare chiaramente quali campi sono "obbligatori" e quali no e quali sono le conseguenze dell'omessa compilazione dei campi obbligatori.
Fonte da cui originano i dati personali.	Dovrebbe essere indicata la fonte specifica dei dati.

Informazioni da fornire all'interessato.	Considerazioni
Esistenza di un processo decisionale automatizzato.	NON APPLICABILE PER UNA IMPRESA DI COSTRUZIONE STANDARD. Va indicato il caso di profilazione e, se del caso, informazioni pregnanti circa la logica seguita e l'importanza e le conseguenze previste del trattamento per gli interessati Si vedano le linee guida del Gruppo su profilazione e processi decisionali automatizzati.

Condizioni di lavoro trasparenti e prevedibili

Il datore di lavoro o il committente, ai sensi del D.Lgs 104/22, è tenuto a informare il lavoratore (in formato cartaceo o elettronico conservando la prova della trasmissione o ricezione per cinque anni dalla conclusione del rapporto di lavoro) circa l'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori.

È necessario fornire informazioni relativamente a:

a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi;
b) gli scopi e le finalità dei sistemi;
c) la logica ed il funzionamento dei sistemi;
d) le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi, inclusi i meccanismi di valutazione delle prestazioni;
e) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità [persona incaricata della corretta applicazione del sistema automatico o decisionale];
f) il livello di accuratezza, robustezza e cybersicurezza dei sistemi e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

Non si ritiene che le aziende standard alle quali sono rivolte queste linee guida utilizzino sistemi decisionali automatizzati (quindi alcune delle informazioni richieste ai punti d) ed e) non risultano pertinenti).

Le altre informazioni dovranno essere ricavate dalla Valutazione d'impatto sulla protezione dei dati prevista dall'art. 35 del RGPD ed obbligatoria per trattamenti che prevedono il monitoraggio automatizzato dei lavoratori.

B. APPENDICE: Liceità dei trattamenti

Riferimenti

Articolo 6 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40)

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43)

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44)

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (C45)

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; (C46)

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46)

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. (C47-C50)

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

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX. (C8, C10, C41, C45, C51)

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: (C8, C10, C41, C45, C51)

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

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

finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: (C50)

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

Articolo 9 - Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (C51)

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52)

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (C55, C56)
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53)

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54)

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (C53)

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. (C8, C10, C41, C45, C53)

Articolo 10 - Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

C. APPENDICE: Il Consenso

Riferimenti

Articolo 7 - Condizioni per il consenso (C42, C43)

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 8 - Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (C38)

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Linee guida sul consenso ai sensi del regolamento

Nel Maggio 2020 sono state adottate dall'European Data Protection Board le "Linee Guida sul consenso ai sensi del regolamento" nelle quali si evidenzia che il consenso può costituire la base legittima appropriata per trattare i dati solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare i termini proposti o rifiutarli senza subire pregiudizio.

Il titolare deve, quindi, valutare se il consenso fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano. In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base valida per il trattamento, rendendo illecita l'attività di trattamento [3[6]].

[6] I numeri fra parentesi quadra permettono il riferimento ai punti del documento originale.

Il fatto che il trattamento si basi sul consenso dell'interessato non fa venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili (Art. 5) ed in particolare non legittima la raccolta di dati non necessari a una finalità specifica di trattamento [5].

Il consenso deve essere la manifestazione di una libera volontà. Se l'interessato non dispone di una scelta effettiva o si sente obbligato ad acconsentire oppure subirà conseguenze negative se non acconsente, il consenso non sarà valido [13].

In particolare, è necessario considerare lo squilibrio di potere che sussiste nel contesto dell'occupazione. Data la dipendenza risultante dal rapporto datore di lavoro/dipendente, è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto. Di conseguenza il Comitato ritiene problematico per il datore di lavoro trattare i dati personali dei dipendenti attuali o futuri sulla base del consenso, in quanto è improbabile che questo venga prestato liberamente. Per la maggior parte delle attività di trattamento svolte sul posto di lavoro, la base legittima non può e non dovrebbe essere il consenso del dipendente in considerazione della natura del rapporto tra datore di lavoro e dipendente [21].

Dato lo squilibrio di potere tra il datore di lavoro e il suo personale, i dipendenti possono manifestare il loro consenso liberamente soltanto in casi eccezionali, quando non subiranno alcuna ripercussione negativa per il fatto che esprimano il loro consenso o meno [22].

È inopportuno "accorpare" il consenso all'accettazione delle condizioni generali di contratto/servizio [26].

Quando i dati sono "necessari per l'esecuzione di un contratto" la base di liceità non sarà il consenso ma l'espressione deve essere interpretata in maniera rigorosa. È necessario che vi sia un collegamento diretto e obiettivo tra il trattamento dei dati e la finalità dell'esecuzione del contratto [30, 31].

È necessario che l'interessato possa esprimere un consenso separato per distinti trattamenti dei dati personali [43]. Il consenso può coprire trattamenti distinti, purché abbiano la medesima finalità [57].

Se il titolare tratta i dati basandosi sul consenso e intende trattarli per un'altra finalità, deve richiedere un ulteriore consenso per tale finalità a meno che non possa basarsi su un'altra base legittima che risponda meglio alla situazione [58].

Fornire informazioni agli interessati prima di ottenerne il consenso è fondamentale per consentire loro di prendere decisioni informate, capire a cosa stanno acconsentendo e, ad esempio, esercitare il diritto di revocare il consenso. Se il titolare del trattamento non fornisce informazioni accessibili, il controllo dell'utente diventa illusorio e il consenso non costituirà una base valida per il trattamento [62].

Quando richiede il consenso, il titolare dovrebbe assicurarsi di usare sempre un linguaggio chiaro e semplice. Ciò significa che il messaggio dovrebbe essere facilmente comprensibile per una persona media, non solo per un avvocato. Il titolare del trattamento non può usare lunghe politiche sulla tutela della vita privata difficili da comprendere oppure informative piene di gergo giuridico. Il consenso deve essere chiaro e distinguibile dalle altre questioni, e deve essere presentato in una forma intelligibile e facilmente accessibile. Ciò significa, in sostanza, che le informazioni pertinenti per prendere una decisione informata sul consenso non possono essere nascoste all'interno delle condizioni generali di contratto/servizio [67].

Se il consenso viene richiesto all'interno di un contratto cartaceo che tratta numerosi aspetti che non sono collegati al consenso all'uso dei dati personali, quest'ultimo deve essere trattato in modo da distinguersi chiaramente oppure in un documento distinto [71].

Il consenso deve sempre essere ottenuto prima che il titolare del trattamento inizi a trattare i dati personali per i quali è necessario il consenso [90].

È necessario che l'utente abbia la possibilità di revocare il consenso con la stessa facilità con cui lo ha espresso [86]. La facilità della revoca è un elemento necessario per considerare valido il consenso. Il titolare deve informare l'interessato del diritto di revoca prima che quest'ultimo presti effettivamente il consenso [116].

Il titolare, per trattamenti che si basano sul consenso, deve essere preparato a interromperli in caso di revoca del consenso. Il titolare non può passare dal consenso ad altre basi legittime (ad esempio non può ricorrere retroattivamente alla base dell'interesse legittimo in caso di problemi di validità del consenso) poiché ha l'obbligo di comunicare la base legittima al momento della raccolta dei dati personali [122, 123].

D. APPENDICE: Parere sul legittimo interesse del Titolare

Premessa

Il RGPD nei considerando affronta il problema legato al legittimo interesse del titolare nel trattamento dei dati, ad esempio, questo potrebbe sussistere nel caso di rapporti di lavoro e commerciali fra il titolare e gli interessati (47), in particolare all'interno di un gruppo imprenditoriale (48) o per la sicurezza delle reti e dell'informazione (49).

Il Gruppo di lavoro consultivo dell'UE per la protezione dei dati personali e della vita privata ha fornito, a suo tempo, un parere sul concetto di interesse legittimo che prevede che l'interesse legittimo del titolare del trattamento, oppure dei terzi cui vengono comunicati i dati, sia valutato rispetto agli interessi o ai diritti fondamentali dell'interessato. L'esito di questo test comparativo permetterà di stabilire se il legittimo interesse può essere invocato come fondamento giuridico per il trattamento.

Il test dovrà valutare appieno una serie di fattori affinché sia possibile garantire che gli interessi e i diritti fondamentali degli interessati siano tenuti nella debita considerazione. Al tempo stesso, il test comparativo è adattabile, può variare da semplice a complesso e non deve risultare indebitamente gravoso.

Tra i fattori di cui tenere conto nell'esecuzione del test comparativo figurano:

- la natura e l'origine dell'interesse legittimo;
- l'impatto sugli interessati e le loro ragionevoli aspettative su ciò che accadrà ai loro dati, nonché la natura dei dati e le modalità di trattamento;
- le garanzie supplementari che potrebbero limitare l'indebito impatto sull'interessato, quali la minimizzazione dei dati, le tecnologie di rafforzamento della tutela della vita privata, una maggiore trasparenza, il diritto all'opposizione e la portabilità dei dati.

Anche se il legittimo interesse fornisce il fondamento giuridico appropriato per il trattamento non esonera dagli obblighi di necessità e proporzionalità. Questo significa che occorre valutare se esistono altri mezzi meno invasivi per conseguire lo stesso obiettivo.

Interesse del Titolare e degli Interessati

L'interesse che il Titolare può avere nel trattamento oppure il beneficio che il responsabile trae (o che potrebbe trarre la società) dal trattamento deve essere articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del Titolare rispetto agli interessi e ai diritti fondamentali dell'interessato. Inoltre, l'interesse in questione deve anche essere concreto ed effettivo, qualcosa che corrisponda alle attività in corso o ai benefici previsti nell'immediato futuro. In altre parole, gli interessi che sono troppo vaghi o teorici non saranno sufficienti.

Il riferimento a "gli interessi o i diritti e le libertà fondamentali dell'interessato" garantisce una maggiore protezione dell'interessato. Se l'interesse perseguito dal Titolare non è preminente rispetto all'interesse e ai diritti dell'interessato, questi prevalgano rispetto al legittimo, ma meno importante~~,~~ interesse del Titolare, a meno che l'impatto del trattamento sugli interessati sia scarsamente rilevante.

Test comparativo

L'interesse legittimo può avere diversi gradi di rilevanza: da irrilevante a piuttosto importante fino a preminente. Analogamente, l'impatto sull'interesse e sui diritti degli interessati può essere più o meno rilevante e andare da poco importante a molto significativo.

L'interesse legittimo del Titolare, quando è poco rilevante e scarsamente preminente può, in generale, prevalere rispetto all'interesse e ai diritti degli interessati solo nei casi in cui l'impatto su tali diritti e interessi sia ancora più irrilevante. D'altro canto, un interesse legittimo importante e preminente può, in alcuni casi e fatte salve determinate garanzie e misure, giustificare anche una notevole ingerenza nella vita privata oppure un altro impatto considerevole sugli interessi o sui diritti degli interessati.

A tale proposito è importante sottolineare il ruolo speciale che possono svolgere le garanzie nella riduzione dell'indebito impatto sugli interessati, modificando in tal modo l'equilibrio tra i diritti e gli interessi in misura tale che l'interesse legittimo degli interessati non prevalga sull'interesse legittimo del Titolare. Il solo utilizzo delle garanzie non è ovviamente sufficiente a giustificare qualsiasi tipo di trattamento in qualunque contesto. Inoltre, le garanzie in questione devono essere adeguate e sufficienti e devono indiscutibilmente e significativamente ridurre l'impatto sugli interessati.

Il test comparativo deve considerare:

- valutazione dell'interesse legittimo del responsabile del trattamento;
- l'impatto sugli interessati;
- bilanciamento provvisorio;
- garanzie supplementari applicate dal Titolare per evitare qualsiasi indebito impatto sugli interessati.

Valutazione dell'Impatto

Nel valutare l'impatto del trattamento, occorre considerare le conseguenze sia positive che negative. Queste possono comprendere potenziali azioni o decisioni future di terzi nonché situazioni in cui il trattamento potrebbe comportare l'esclusione o la discriminazione di persone, la diffamazione o, in senso più ampio, situazioni in cui esiste il rischio di danneggiare la reputazione, il potere negoziale o l'autonomia dell'interessato.

Oltre a esiti negativi che possono essere specificamente previsti, occorre tenere conto anche delle più ampie conseguenze emotive, quali l'irritazione, la paura e l'ansia che può provare un interessato che non abbia più il controllo dei suoi dati personali o che si sia reso conto che tali informazioni sono state o possono essere utilizzate in maniera impropria o compromesse, per esempio mediante l'esposizione su Internet. Occorre tenere nella debita considerazione anche l'effetto dissuasivo sui comportamenti protetti, quali la libertà di ricerca o la libertà di espressione, che potrebbe derivare da continue attività di monitoraggio/tracciamento.

La valutazione dell'impatto potenziale dovrà tenere in conto la probabilità che il rischio si concretizzi e la gravità delle conseguenze.

Andrà quindi valutata la natura dei dati ponendo particolare attenzione qualora vengano trattate categorie particolari di dati (ex dati sensibili).

In generale, quanto più negativo o incerto potrà essere l'impatto del trattamento (numero di persone che possono accedere ai dati, eventuale combinazione con altri dati, ecc.), tanto più sarà improbabile che, nel complesso, il trattamento sia considerato legittimo.

Le ragionevoli aspettative dell'interessato riguardo all'utilizzo e alla comunicazione dei dati sono anch'esse estremamente pertinenti a questo riguardo.

È necessario esaminare se esiste uno squilibrio nella relazione tra la posizione dell'interessato e quella del Titolare (es. Lavoratore / Datore di lavoro).

Il Titolare potrebbe valutare la possibilità di introdurre misure supplementari, che vadano oltre il rispetto delle disposizioni generali del RGPD, per contribuire a ridurre l'indebito impatto del trattamento sugli interessati.

Ad esempio, rigorose limitazioni della quantità di dati raccolti e l'immediata cancellazione dei dati dopo il loro utilizzo, la pseudonimizzazione e la cifratura, analogamente a qualsiasi altra misura tecnica e organizzativa introdotta a tutela dei dati personali, svolgeranno un ruolo importante

riguardo alla valutazione del potenziale impatto del trattamento sull'interessato e, di conseguenza, in alcuni casi potrebbero contribuire a far pendere il bilanciamento a favore del Titolare. L'utilizzo di forme meno rischiose di trattamento dei dati personali (quali ad esempio la cifratura di dati personali in fase di conservazione o di transito oppure dati personali che sono meno direttamente e meno immediatamente identificabili) deve in generale significare che esistono minori probabilità di ingerenze negli interessi o nei diritti e nelle libertà fondamentali degli interessati.

Tra le misure supplementari potrebbe figurare, per esempio, la disponibilità di un meccanismo facilmente accessibile ed efficace volto ad assicurare agli interessati la possibilità incondizionata di opporsi al trattamento dei dati. In alcuni casi (ma non in tutti) queste misure supplementari potrebbero contribuire a far pendere il bilanciamento in un senso o nell'altro e a garantire che il trattamento possa basarsi sul "legittimo interesse", tutelando al contempo anche i diritti e gli interessi degli interessati.

Misure supplementari possono essere:

- rigorosa limitazione della quantità di dati raccolti;
- immediata cancellazione dei dati dopo il loro utilizzo;
- separazione funzionale;
- adozione di tecniche di anonimizzazione;
- maggiore trasparenza;
- diritto generale ed incondizionato ad opporsi in qualsiasi momento al trattamento.

Responsabilità e trasparenza

Come norma di buona pratica è opportuno che l'esecuzione del test sia documentata in maniera sufficientemente dettagliata e trasparente in modo da permettere di verificare la completa e corretta applicazione del test, se del caso, da parte dei soggetti pertinenti, tra cui gli interessati e le autorità di protezione dei dati nonché, in ultima analisi, dei tribunali competenti.

È opportuno che il Titolare spieghi agli interessati, in maniera chiara e semplice, i motivi per cui ritiene che gli interessi o i diritti e le libertà fondamentali degli interessati non prevalgano sui suoi interessi illustrando altresì loro quali garanzie ha adottato per tutelare i dati personali compreso, se del caso, il diritto ad opporsi al trattamento.

Garanzie supplementari

Ai sensi dell'Art. 21 del RGPD l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento in base al legittimo interesse del Titolare dei dati personali che lo riguardano. La richiesta dell'interessato rappresenta una integrazione al test di bilanciamento che richiede una ulteriore valutazione.

La scelta del Titolare di assicurare metodi semplici e non condizionati per consentire l'opposizione al trattamento da parte dell'interessato può favorire la liceità del legittimo interesse.

Anche la disponibilità di meccanismi efficaci volti a permettere agli interessati di accedere ai loro dati, modificarli, cancellarli, o sottoporli ad ulteriori trattamenti può favorire la liceità del legittimo interesse responsabilizzando e aiutando gli interessati a comprendere le potenzialità dei dati trattati.

E. APPENDICE: Designazioni

Riferimenti

Articolo 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione

Articolo 32 - Sicurezza del trattamento

…

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

CODICE: Art. 2-quaterdecies

(Attribuzione di funzioni e compiti a soggetti designati)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

F. APPENDICE: Titolare e Responsabile nel RGPD

Riferimenti

Articolo 28 - Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro

responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10.Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Linee guida sui concetti di Titolare e Responsabile nel RGPD

Nel settembre 2020 lo "European Data Protection Board" ha adottato delle Linee Guida nelle quali sono fornite indicazioni sia su come individuare i Responsabili dei trattamenti sia su come definire i rapporti fra Titolare e Responsabile.

Di seguito vengono riportati fra parentesi quadra numeri che indicano i paragrafi di riferimento nelle Linee Guida.

Oggetto del Trattamento

[111] L'oggetto dell'elaborazione deve essere formulato con sufficienti specifiche in modo che sia chiaro quale sia l'oggetto principale dell'elaborazione (ad esempio, registrazioni di videosorveglianza di persone che entrano ed escono da una struttura ad alta sicurezza).

La natura del trattamento: il tipo di operazioni effettuate nell'ambito del trattamento (ad esempio: "ripresa", "registrazione", "archiviazione di immagini", ...) e la finalità del trattamento (ad esempio: individuazione di un'entrata illecita) devono essere descritte per permettere di comprendere il contenuto e i rischi del trattamento affidato al Responsabile.

È necessario specificare il tipo di dati personali nel modo più dettagliato possibile (ad esempio: immagini video di persone che entrano ed escono dalla struttura). Nel caso di categorie particolari di dati è necessario specificare quali tipi di dati sono interessati (ad esempio, "informazioni relative alle cartelle cliniche", "informazioni sull'appartenenza o meno dell'interessato a un sindacato", …).

Vanno definite in modo preciso le categorie di soggetti interessati (ad esempio: "visitatori", "dipendenti", servizi di consegna, …).

Scelta del Responsabile

[92] Il Titolare ha il dovere di utilizzare solo Responsabili che forniscano garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate.

[93] Le garanzie "fornite" dal Responsabile sono quelle dimostrabili con soddisfazione del Titolare, in quanto sono le uniche che possono essere effettivamente tenute in conto nel valutare il rispetto degli obblighi. Spesso ciò richiede uno scambio di documentazione rilevante (ad es. politica sulla privacy, termini di servizio, registrazione delle attività di elaborazione, politica di gestione dei record, politica di sicurezza delle informazioni, rapporti di audit esterni, certificazioni internazionali riconosciute).

[97] L'obbligo di utilizzare solo Responsabili "che offrano garanzie sufficienti" è un obbligo continuo. Esso non cessa nel momento in cui il Titolare e il Responsabile concludono un contratto. Il Titolare deve piuttosto verificare, a intervalli appropriati, le garanzie del Responsabile, anche mediante audit e ispezioni, se del caso.

Obblighi del Titolare

[109] L'accordo di trattamento non dovrebbe limitarsi a ribadire le disposizioni del RGPD: dovrebbe piuttosto includere informazioni più specifiche e concrete su come saranno soddisfatti i requisiti e sul livello di sicurezza richiesto per il trattamento dei dati personali oggetto dell'accordo di trattamento… [con] una chiara attribuzione delle responsabilità.

[110] Il contratto tra le parti dovrebbe essere redatto alla luce della specifica attività di trattamento dei dati. Ad esempio, non è necessario imporre protezioni e procedure particolarmente rigorose a un Responsabile incaricato di un'attività di trattamento da cui derivano solo rischi minori… le misure e le procedure devono essere adeguate alla situazione specifica.

Il contratto deve includere alcuni elementi che possono aiutare il Responsabile a comprendere i rischi per i diritti e le libertà degli interessati derivanti dal trattamento [di cui] il Titolare ha una comprensione più approfondita, poiché è consapevole delle circostanze in cui esso è incorporato.

[113] Il Titolare deve fornire al Responsabile istruzioni relative a ciascuna attività di elaborazione. Tali istruzioni possono comprendere il trattamento consentito e non consentito dei dati personali, procedure più dettagliate, modalità di sicurezza dei dati, ecc. Il Responsabile non deve andare oltre quanto indicato dal responsabile del trattamento.

[115] Le istruzioni devono essere documentate (esempio: una procedura e un modello per fornire ulteriori istruzioni in un allegato) e conservate insieme al contratto.

Controllo sulle attività del Responsabile

[117] Il Titolare [deve prestare particolare attenzione ai trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale], specialmente quando il Responsabile sta per delegare alcune attività di elaborazione ad altri Responsabili, e quando il Responsabile ha divisioni o unità situate in paesi terzi.

[38] I "mezzi essenziali" sono strettamente legati allo scopo e alla portata dell'elaborazione e sono tradizionalmente e intrinsecamente riservati al Titolare. Esempi di mezzi essenziali sono il tipo di dati personali che vengono trattati ("quali dati saranno trattati?"), la durata del trattamento ("per quanto tempo saranno trattati? "), le categorie di destinatari ("chi vi ha accesso? ") e le categorie di soggetti interessati ("i cui dati personali sono trattati?").

I "mezzi non essenziali" riguardano aspetti più pratici dell'attuazione, come la scelta di un particolare tipo di hardware o software o le misure di sicurezza dettagliate che possono essere lasciate alla decisione del Responsabile.

[119] Il Titolare deve garantire la riservatezza dei dati personali a chiunque consenta di trattarli.

[130] Il contratto non deve limitarsi a ribadire gli obblighi di assistenza. Deve contenere dettagli su come si chiede al Responsabile di aiutare il Titolare a rispettare gli obblighi elencati.

Ad esempio, negli allegati all'accordo possono essere aggiunti procedure e modelli di formulari che consentano al Responsabile di fornire al Titolare tutte le informazioni necessarie.

[131] Il Titolare deve informare adeguatamente il Responsabile in merito al rischio connesso al trattamento e a qualsiasi altra circostanza che possa aiutare il Responsabile a svolgere il suo compito.

[127] Il contratto deve prevedere che il Responsabile abbia l'obbligo di fornire assistenza [per le richieste degli interessati]. La natura di tale assistenza può variare notevolmente "tenendo conto della natura del trattamento" e in funzione del tipo di attività affidata al Responsabile dal Titolare. I dettagli relativi all'assistenza che l'incaricato del trattamento deve fornire devono essere inclusi nel contratto o in un suo allegato.

[129] La valutazione dell'ammissibilità delle richieste degli interessati e/o del rispetto dei requisiti stabiliti dal RGPD deve essere effettuata dal Titolare, caso per caso o mediante chiare istruzioni fornite al Responsabile nel contratto prima dell'inizio del trattamento. Inoltre, i termini stabiliti dal capo III non possono essere prorogati dal Titolare in base al fatto che le informazioni necessarie devono essere fornite dal Responsabile.

[133] Il Responsabile deve assistere il Titolare nell'adempimento dell'obbligo di notificare le violazioni dei dati personali ... Il Responsabile deve fornire informazioni al Titolare ogni volta che scopre una violazione dei dati personali che interessa le strutture / i sistemi informatici [suoi] o di un sub Responsabile e aiutare il Titolare a ottenere le informazioni che devono essere indicate nella relazione all'autorità di controllo.

Il RGPD richiede che il Titolare notifichi una violazione senza indebiti ritardi … Pertanto, anche la comunicazione del Responsabile al Titolare deve avvenire senza indebiti ritardi. L'EDPB raccomanda di prevedere nel contratto un determinato periodo di tempo per la notifica (ad esempio il numero di ore) e di indicare il punto di contatto per tale notifica. Il contratto dovrebbe infine specificare come il Responsabile del trattamento deve notificare al Titolare del trattamento in caso di violazione.

Subresponsabili

[125] L'accordo deve specificare che il Responsabile non può impegnare un altro Responsabile senza previa autorizzazione scritta del Titolare e se tale autorizzazione sarà specifica o generale.

[148] Anche se le attività di elaborazione dei dati sono spesso svolte da un gran numero di attori e le catene di subappalto diventano sempre più complesse, il Titolare mantiene il suo ruolo fondamentale nel determinare lo scopo e i mezzi di elaborazione.

[153] Pertanto, la differenza principale tra l'autorizzazione specifica e gli scenari di autorizzazione generale sta nel significato dato al silenzio del Titolare: nella situazione di autorizzazione generale, la mancata obiezione entro il termine stabilito può essere interpretato come autorizzazione.

Attività a conclusione del Contratto

[137] Il Titolare può decidere all'inizio se i dati personali devono essere cancellati o restituiti specificandolo nel contratto.

[138] Se il Titolare sceglie di cancellare i dati personali, il Responsabile deve garantire che la cancellazione sia effettuata in modo sicuro. Il Responsabile deve confermare al Titolare che la cancellazione è stata completata entro un termine concordato e secondo modalità concordate.

Misure di sicurezza

[123] Il contratto deve contenere o fare riferimento a informazioni relative alle misure di sicurezza da adottare, all'obbligo per il Responsabile di ottenere il visto del Titolare prima di apportare modifiche e a una revisione periodica delle misure di sicurezza in modo da garantirne l'adeguatezza rispetto ai rischi, che possono evolvere nel tempo.

Il grado di dettaglio delle informazioni relative alle misure di sicurezza da includere nel contratto deve essere tale da consentire al Titolare di valutare l'adeguatezza delle misure ai sensi dell'articolo 32, paragrafo 1.

[124] Il livello di istruzioni fornite dal Titolare al Responsabile per quanto riguarda le misure da attuare dipenderà dalle circostanze specifiche.

In alcuni casi, il Titolare può fornire una descrizione chiara e dettagliata delle misure di sicurezza da attuare.

In altri casi, il Titolare può descrivere gli obiettivi minimi di sicurezza da raggiungere, chiedendo al Responsabile di proporre l'attuazione di specifiche misure di sicurezza.

In ogni caso, il Titolare deve fornire al Responsabile una descrizione delle attività di trattamento e degli obiettivi di sicurezza (sulla base della valutazione dei rischi del Titolare), nonché approvare le misure proposte dal Responsabile. Ciò potrebbe essere incluso in un allegato al contratto.

Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021

Nella Gazzetta ufficiale dell'Unione Europea del 7 giugno 2021 sono state pubblicate le "*clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio*".

Ai fini delle presenti Linee Guida il "Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati" non risulta di interesse.

I trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri. Il titolare del trattamento e il responsabile del trattamento possono scegliere di negoziare un contratto individuale contenente gli elementi obbligatori di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679, oppure di utilizzare, in tutto o in parte, le clausole contrattuali tipo adottate dalla Commissione in conformità dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679.

Il titolare del trattamento e il responsabile del trattamento dovrebbero essere liberi di includere le clausole contrattuali tipo stabilite nella decisione in oggetto in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo o pregiudichino i diritti o le libertà fondamentali degli interessati. L'utilizzo delle clausole contrattuali tipo lascia impregiudicato qualunque obbligo contrattuale del titolare del trattamento e/o del responsabile del trattamento di garantire il rispetto dei privilegi e delle immunità applicabili.

G. APPENDICE: Registro delle attività di trattamento

Riferimenti

Articolo 30 - Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

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) 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 e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

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 di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

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 e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Quando è obbligatorio tenere il Registro delle attività di trattamento

La tenuta del Registro della attività di trattamento, consigliata per tutte le imprese, è obbligatoria per le imprese o organizzazioni con almeno 250 dipendenti e in tutti i casi in cui il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato o il trattamento non sia occasionale

o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Modello di "registro semplificato" attività di trattamento del titolare per PMI

Il Garante per la protezione dei dati personali ha messo a disposizione sul proprio sito le istruzioni sul Registro delle attività di trattamento, previsto dal Regolamento (EU) n. 679/2016 (di seguito "RGPD").

Il Registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Come specificato nelle FAQ del Garante è tenuto a redigere il Registro, tra l'altro, qualunque titolare che effettui trattamenti che possano presentare rischi, anche non elevati, per i diritti e le libertà delle persone o che effettui trattamenti non occasionali di dati oppure trattamenti di particolari categorie di dati (come i dati biometrici, dati genetici, quelli sulla salute, sulle convinzioni religiose, sull'origine etnica etc.), o anche di dati relativi a condanne penali e a reati.

Nelle FAQ vengono indicate, tra l'altro, quali informazioni deve contenere il Registro e le modalità per la sua conservazione e il suo aggiornamento. Ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento.

Il Garante ha inoltre fornito un esempio di Registro semplificato.

H. APPENDICE: Trattamento dei dati personali dei lavoratori

Riferimenti

Articolo 88 - Trattamento dei dati nell'ambito dei rapporti di lavoro (C155)

1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Riferimenti presenti nel Codice per la protezione dei dati personali

Capo II -Trattamento di dati riguardanti i prestatori di lavoro

Art. 113 Raccolta di dati e pertinenza

Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n.300 nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276.

Capo III - Controllo a distanza, lavoro agile e telelavoro

Art. 114 (Garanzie in materia di controllo a distanza)

Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300.

Art. 115 (Telelavoro, lavoro agile e lavoro domestico)

1. Nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

Statuto dei Lavoratori: 300/70

Art. 4. (Impianti audiovisivi e altri strumenti di controllo).

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, 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 e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della 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. I provvedimenti di cui al terzo periodo sono definitivi.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Art. 8. (Divieto di indagini sulle opinioni)

È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

D.lgs. 276/03 – Attuazione delle deleghe in materia di occupazione e mercato del lavoro

Art. 10. (Divieto di indagini sulle opinioni e trattamenti discriminatori)

1. È fatto divieto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento dell'attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. È altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

2. Le disposizioni di cui al comma 1 non possono in ogni caso impedire ai soggetti di cui al medesimo comma 1 di fornire specifici servizi o azioni mirate per assistere le categorie di lavoratori svantaggiati nella ricerca di una occupazione.

Provvedimenti del Garante

Controlli in ambito lavorativo

NOTA: Di seguito vengono riportati alcuni estratti da provvedimenti del Garante per la protezione dei dati personali che possono essere di interesse per comprendere limiti che devono essere rispettati nei controlli in ambito lavorativo. Essendo provvedimenti relativi a casi specifici devono essere contestualizzati ma possono fornire valide indicazioni ai Titolari.

Conformemente al costante orientamento della Corte europea dei diritti dell'uomo, **la protezione della vita privata si estende anche all'ambito lavorativo**, considerato che proprio in occasione dello svolgimento di attività lavorative e/o professionali si sviluppano relazioni dove si esplica la personalità del lavoratore (v. artt. 2 e 41, comma 2, Cost). [WEB 9518890][7]

La linea di confine tra ambito lavorativo e professionale e quello strettamente privato non può sempre essere tracciata in modo netto, **non può essere prefigurato l'annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro**, anche nei casi in cui il dipendente sia connesso ai servizi di rete messi a disposizione del datore di lavoro o utilizzi una risorsa aziendale anche attraverso dispositivi personali, ragione per la quale la Corte europea dei diritti dell'uomo, ha nel tempo confermato che la protezione della vita privata (art. 8 Convenzione europea dei diritti dell'Uomo) si estende anche all'ambito lavorativo, ove si esplicano la personalità e le relazioni della persona che lavora[8]. Pertanto, il trattamento dei dati effettuato mediante tecnologie informatiche, nell'ambito del rapporto di lavoro, deve conformarsi al rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, a tutela di lavoratori e di terzi[9]. [WEB 9669974]

L'ambito dei controlli (indiretti o preterintenzionali), entro i limiti stabiliti dalla disciplina di settore, e i trattamenti di dati personali che possono essere lecitamente effettuati dal datore di lavoro, **devono essere comunque non massivi, graduali e ammissibili solo previo esperimento di misure meno limitative dei diritti lavoratori[10]**. [WEB 9669974]

[Non] può essere ritenuto sufficiente che il datore di lavoro si limiti a richiamare il corretto utilizzo degli strumenti di rete da parte dei propri dipendenti (es: "è di fondamentale importanza che il lavoratore si attenga rigorosamente alle istruzioni per l'utilizzo degli strumenti informatici affinché non [possano essere rilevate] informazioni che attengono alla Sua sfera privata extraprofessionale, e/o alle categorie di dati di cui agli artt. 9 e 10 del RGPD 2016/679""), facendo

[7] Fra parentesi quadre, dopo la sigla WEB, sono riportati i riferimenti ai documenti web scaricabili dal sito del Garante Italiano.

[8] v. Sentenze della Corte Europea dei Diritti dell'Uomo Niemietz c. Allemagne, 16.12.1992 (ric. n. 13710/88), spec. par. 29; Copland v. UK, 03.04.2007 (ric. n. 62617/00), spec. par. 41; Bărbulescu v. Romania [GC], 5.9.2017 (ric. n. 61496/08), spec. parr. 70-73 e 80; Antović and Mirković v. Montenegro, 28.11. 2017 (ric. n. 70838/13), spec. par. 41-42

[9] v. Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, spec. punto 3

[10] cfr. Audizione del Garante sul Jobs Act presso Commissione lavoro Camera deputati 9 luglio 2015, doc. web n. 4119045; nonché "Dichiarazione di Antonello Soro, Presidente del Garante per la privacy, su sentenza Corte di Strasburgo" - CEDU, sentenza 17 ottobre 2019, López Ribalda and others v. Spain-, doc. web n. 9164334, "il requisito essenziale perché i controlli sul lavoro, anche quelli difensivi, siano legittimi resta dunque, per la Corte, la loro rigorosa proporzionalità e non eccedenza: capisaldi della disciplina di protezione dati la cui "funzione sociale" si conferma, anche sotto questo profilo, sempre più centrale perché capace di coniugare dignità e iniziativa economica, libertà e tecnica, garanzie e doveri"

leva esclusivamente sulla responsabilità dei dipendenti e sul divieto di utilizzo degli strumenti informativi per fini personali. [WEB 9669974]

Informazioni ai lavoratori

Atti redatti per assolvere ad obblighi diversi rispetto a quelli derivanti dalla disciplina in materia di protezione dei dati (quali un codice di comportamento, circolari interne, un eventuale accordo sindacale, ecc.) che non contengano tutti gli elementi informativi essenziali richiesti dall'art. 13 del Regolamento **non possono sostituire l'informativa** che il titolare deve rendere, prima di iniziare il trattamento agli interessati in merito alle caratteristiche essenziali dello stesso.

L'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica condizione per il **lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro**, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. 20 maggio 1970, n. 300). [WEB 9669974]

L'approccio di fornire agli interessati **informative stratificate** è utile ai fini del rispetto del principio di trasparenza **solo se le informazioni di primo e di secondo livello sono presentate tra loro in maniera coerente e strutturata**, consentendo agli interessati di conoscere gli elementi essenziali del trattamento nella prima informativa di primo livello, potendo poi scegliere di approfondire determinati aspetti nelle informative di dettaglio[11]. [WEB 9703988]

Utilizzo di caselle di posta elettronica individualizzate

Il datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità ([12]si veda in proposito Cass. 31.3.2016, n. 13057, laddove si afferma che **qualora "siano attivate caselle di posta elettronica – protette da password personalizzate – a nome di uno specifico dipendente, quelle «caselle» rappresentano il domicilio informatico proprio del dipendente […]. La casella rappresenta uno «spazio» a disposizione – in via esclusiva – della persona, sicché la sua invasione costituisce, al contempo, lesione della riservatezza"**). Tanto più che l'assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione[13]. [WEB 8159221]

Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, **gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi**

[11] sul punto, "Linee guida sulla trasparenza ai sensi del regolamento 2016/67" adottate l'11 aprile 2018, WP260 rev.01, par. 35, successivamente fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018: "le dichiarazioni/informative sulla privacy non sono mere pagine annidiate in altre che richiedono diversi clic per arrivare all'informazione voluta: il design e il layout del primo strato della dichiarazione/informativa sulla privacy dovrebbe essere tale da offrire all'interessato una panoramica chiara delle informazioni a sua disposizione sul trattamento dei dati personali e del luogo e del modo in cui può trovarle fra i diversi strati"

[12] v., tra gli altri, Provv. n. 139 del 7 aprile 2011, doc. web n. 1812154; Provv. n. 308 del 21.7.2011, doc. web n. 1829641; Provv. 23 dicembre 2010, doc. web n. 1786116.

[13] cfr. Provv. 1° marzo 2007, n. 13, "Linee guida per posta elettronica e internet", spec. 3; 5.2. lett. b), e 6.1.

riferiti all´attività professionale del titolare del trattamento. L´interesse del titolare ad accedere alle informazioni necessarie all´efficiente gestione della propria attività, pertanto, deve essere contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi[14]. [WEB 8159221]

La conservazione sistematica dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli account aziendali, allo scopo di poter ricostruire gli scambi di comunicazioni tra gli uffici interni nonché tutti i rapporti intrattenuti con gli interlocutori esterni (clienti, fornitori, enti assicurativi, tour operator), anche in vista di possibili contenziosi, effettuata da soggetti diversi dal titolare della specifica casella di posta elettronica per l´intera durata del rapporto di lavoro e successivamente all´interruzione dello stesso, **non risulta altresì conforme ai principi di liceità, necessità e proporzionalità del trattamento** (v. artt. 3, 11, comma 1, lett. a) e d) del Codice).

La legittima necessità di assicurare l´ordinario svolgimento e la continuità dell´attività aziendale nonché di provvedere alla dovuta conservazione di documentazione in base a specifiche disposizioni dell´ordinamento è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali - attraverso l´adozione di appropriate misure organizzative e tecnologiche - individuare i documenti che nel corso dello svolgimento dell´attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile[15]. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche. [WEB 8159221]

Il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione - avanzata dalla società - risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento[16]. [WEB 8159221]

Al database [di posta elettronica] relativo al singolo account può avere accesso (anche effettuando le operazioni consentite dal sistema) solo l'interessato, intestatario dell'account stesso. Resta fermo altresì che in relazione alle attività di raccolta e conservazione necessarie a consentire le operazioni di trattamento da parte dell'interessato, il titolare è tenuto ad osservare quanto stabilito dall'Autorità con il Provvedimento 27 novembre 2008 sugli amministratori di sistema. [WEB 8159221]

Non è lecito che il superiore gerarchico o qualunque altro dipendente (benché "sentito" l'interessato) possa **accedere alla casella di posta individualizzata in relazione ad una indefinita pluralità di scopi** [WEB 9518890].

La possibilità per la società di **accedere** sia ai dati esterni che **al contenuto delle caselle email in costanza del rapporto di lavoro, comporta un trattamento di dati personali illecito** in violazione

[14] v. provv.ti 30 luglio 2015, n. 456, doc. web n. 4298277; 5 marzo 2015, n. 136, doc. web n. 3985524 e 27 novembre 2014, n. 551, doc. web n. 3718714

[15] si veda quanto stabilito dal D.P.C.M. 3 dicembre 2013, recante le Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell´amministrazione digitale di cui al decreto legislativo n. 82 del 2005; parimenti i documenti che rivestano la qualità di "scritture contabili" devono essere memorizzati e conservati con modalità determinate: artt. 2214 c.c.; artt. 43 e 44, d. lgs. 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale"

[16] v. artt. 23 e 24 del Codice; si vedano anche i provv.ti 19 marzo 2015, doc. web n. 4039439, 20 febbraio 2014, doc. web n. 3115239 e 4 giugno 2009, doc. web n. 1629029

dell'art. 4, l. 20.5.1970, n. 300, richiamato dall'art. 114 del Codice come condizione di liceità del trattamento (esercitando un controllo sull'attività del lavoratore), nonché la possibilità di accedere ad informazioni relative all'interessato non rilevanti, in violazione dell'art. 8, l. 20.5.1970, n. 300 e dell'art. 10 del d.lgs.10.9.2003, n. 276, richiamati dall'art. 113 del Codice come condizione di liceità del trattamento (contenenti il divieto di effettuare indagini o comunque trattare dati che non siano strettamente attinenti alla valutazione dell'attitudine professionale del dipendente). Tale disciplina lavoristica costituisce una delle norme del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" individuate dall'art. 88 del Regolamento (e, come misura appropriata e specifica ai sensi del par. 2 del medesimo art. 88, non consente controlli massivi, prolungati e indiscriminati dell'attività del dipendente). [WEB 9518890]

"**Grava […] sul datore di lavoro l'onere di indicare […], chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli**"[17].

In capo al titolare del trattamento vi è, quindi, l'obbligo di fornire una preventiva informativa all'interessato in ordine alle caratteristiche essenziali dei trattamenti effettuati.

Si ricorda, peraltro, che non è possibile effettuare un controllo, da parte del datore di lavoro, in violazione di quanto previsto dall'art. 4 della L. n. 300 del 1970 richiamato dall'art. 114 del Codice.

L'Autorità si è pronunciata sulle condizioni di liceità di alcuni trattamenti di dati tratti dall'utilizzo di strumenti di lavoro, tra cui la posta elettronica, per finalità di sicurezza dei sistemi e di gestione dei servizi (v. Provv. n. 303 del 13.7.2016, doc. web n. 5408460, spec. par. 4.2., 4.3. e 5, anche con riferimento ai tempi di conservazione, con il quale sono stati indicati tra i "sistemi e le misure che […] consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore" i "sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una breve durata non superiore comunque ai sette giorni"). [WEB 8159221]

Controlli sulla navigazione

Il MAC Address della "interfaccia" di rete di una postazione è da considerarsi "dato personale" ai sensi della disciplina comunitaria e nazionale in materia di protezione dei dati (art. 4, comma 1, lett. b) del Codice). Infatti, il MAC Address è costituito da una sequenza numerica (48 cifre binarie) associata in modo univoco dal produttore a ogni scheda di rete ethernet o wireless prodotta al mondo e rappresenta l´indirizzo fisico identificativo di quel particolare dispositivo di rete da cui è possibile desumere l´identità del produttore, la tipologia di dispositivo e, in taluni casi, anche risalire all´acquirente o utilizzatore dell´apparato: è infatti sostanzialmente immodificabile e, date le caratteristiche (in particolare, la sua univocità su scala globale), consente di risalire, anche indirettamente, alla postazione corrispondente e di conseguenza all´utente che su di essa sta operando. Per tutto ciò il suo trattamento impone il rispetto della normativa sulla protezione dei dati personali[18].

[17] In base agli articoli 11, comma 1, lett. a) e 13 del Codice; cfr. anche Provv. 1° marzo 2007, n. 13, "Linee guida per posta elettronica e internet", spec. punto 3.1, medesime conclusioni in European Court of Human Rights, Grand Chamber, case of Bărbulescu v. Romania, Application no. 61496/08, 5 September 2017, spec. n. 140.

[18] cfr., Gruppo Art. 29, Parere n. 4/2007 - WP 136 sul concetto di dato personale; sul carattere di dato personale del MAC Address stante la relativa univocità, cfr. Gruppo Art. 29, Parere n. 13/2011 - WP 185 sui servizi di geolocalizzazione su dispositivi mobili intelligenti, spec. p. 11; segnalazione del Garante a Governo e Parlamento del 9 luglio 2013 con particolare riferimento all´art. 10, d.l. n. 69 del 21 giugno 2013. c.d. "decreto del fare"; Provv.ti 10

Il trattamento di dati effettuato attraverso operazioni di controllo, filtraggio, monitoraggio e tracciatura delle connessioni e dei collegamenti ai siti internet esterni, registrati in modo sistematico e conservati per un ampio arco temporale, è idoneo a consentire un controllo dell'attività e dell'utilizzo dei servizi della rete individualmente effettuato da soggetti identificabili. Ciò, nei casi in cui il trattamento sia posto in essere nei confronti dei dipendenti e in presenza di collegamento tra i dati relativi alla connessione e la persona utilizzatrice, consente di ricostruirne anche indirettamente l'attività e **risulta in contrasto con il principio di liceità nonché con la rilevante disciplina di settore in materia di lavoro.** [WEB 5408460]

Eventuali trattamenti effettuati per il tramite di apparati (differenti dalle ordinarie postazioni di lavoro) **e di sistemi software che consentono**, con modalità non percepibili dall´utente (c.d. in background) e in modo del tutto indipendente rispetto alla normale attività dell´utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente), **operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati degli accessi a Internet o al servizio di posta elettronica non possono essere considerati "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"** (ai sensi e per gli effetti dell´art. 4, comma 2, l. n. 300/1970, come modificato dall´art. 23 del d.lg. n. 151/2015[19]).

In tale nozione, infatti - e con riferimento agli strumenti di posta elettronica e navigazione web - è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. **Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore** (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con **conservazione dei soli dati esteriori**, contenuti nella cosiddetta "envelope" del messaggio, **per una breve durata non superiore comunque ai sette giorni**; sistemi di **filtraggio anti-virus** che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l´erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso). [WEB 5408460]

La raccolta sistematica dei dati di navigazione dei dipendenti comporta inevitabilmente il trattamento di informazioni anche estranee all'attività professionale, desumibili dagli URL visitati, e risulta, pertanto, **in contrasto con il divieto per il datore di lavoro di trattare dati "non attinenti alla valutazione dell'attitudine professionale del lavoratore"** e dunque con l'art. 113 del Codice, in riferimento all'art. 8 della l. 20 maggio 1970, n. 300 e all'art. 10 del d.lgs. 10 settembre 2003, n. 276[20]. Non è necessario sottoporre i dati raccolti ad alcun particolare trattamento per incorrere nell'illecito, poiché **la mera acquisizione e conservazione della disponibilità di essi comporta la violazione della prescrizione legislativa**.

---

luglio 2014, doc. web n. 3283078, spec. punto 2; 19 marzo 2015, doc. web n. 3881513, punto 3; 12.03.2015, doc. web n. 3881392; 23.04.2015, doc web n. 4015426

[19] sul punto, cfr. nota del Ministero del Lavoro e delle Politiche Sociali, del 18 giugno 2015; v. altresì la definizione di "attrezzatura" e "postazione di lavoro" di cui all´art. 173 d.lg. n. 81/2008.

[20] cfr., sul punto Provv. del Garante n. 308 del 21 luglio 2011, doc. web n. 1829641, confermato da Corte di Cassazione, sent. n. 18302 del 19 settembre 2016, ove si legge che "l'acquisizione e conservazione dei dati relativi alla navigazione Internet dei dipendenti mediante […] registrazione dei file log importa la violazione anche del disposto di cui alla legge n. 300 del 1970, art. 8" e che "acquisire e conservare dati che contengono (o possono contenere) simili informazioni comporta già l'integrazione della condotta vietata […] anche se i dati non sono successivamente utilizzati.

La possibilità di intraprendere rilevazioni di dati puntuali di navigazione in internet, [è possibile] **solo a fronte di riscontrate anomalie di traffico web la cui entità sia tale da compromettere la sicurezza e l'integrità dei sistemi informativi** [e solo secondo quanto previsto da specifiche procedure aziendali previo accordo sindacale]. [WEB 9669974]

Tempi di conservazione dei dati

Di seguito vengono riportati i termini per alcune azioni.

Elemento	Riferimento	Termini
Azione di regresso INAIL per il rimborso di quanto erogato al lavoratore per infortunio malattia	Articolo 112, comma 5, DPR 1124/1955. Decorrenti alla conclusione del procedimento penale a carico del datore di lavoro o, se questo non è stato iniziato dalla, liquidazione dell'indennizzo il danneggiato.	3 anni
Somme pagate con periodicità annuale o inferiore (ad esempio l'attribuzione mensile) compresi gli interessi su tali somme.	Articolo 2948, n. 4 Codice civile. La prescrizione decorre durante il rapporto di lavoro solo ove questo sia assistito dalla stabilità (Corte costituzionale 12 dicembre 1972, n. 174).	5 anni
Trattamento di fine rapporto ed altre indennità spettanti per la cessazione del rapporto.	Articolo 2948, n. 5 Codice civile. La prescrizione decorre dalla data della cessazione del rapporto di lavoro.	5 anni
Azioni di annullamento di un atto unilaterale (ad esempio: dimissioni, rinuncia, ecc.).	Articolo 1442 Codice civile	5 anni
Azione di risarcimento per fatto illecito extracontrattuale.	Articolo2947, c. 1 e 2 Codice civile. La prescrizione decorre dal giorno in cui il fatto si è verificato.	5 anni
Azioni per crediti contributivi senza denuncia da parte del lavoratore all'INPS.	Articolo 3, c. 9 e 10, Legge 335/1995.	5 anni
Segnalazioni di violazioni	Art. 14 comma 1 del D.Lgs 24/2023.	5 anni
Azione di risarcimento contrattuale (ad esempio in caso di licenziamento legittimo o per mancata fruizione delle ferie o del riposo settimanale, danno all'integrità psicofisica del lavoratore).	Articolo 2946 Codice civile.	10 anni
Azione per crediti contributivi con denuncia di omissione contributiva presentata dal lavoratore o da suoi eredi all'INPS entro 5 anni.	Articolo 3, c. 9 e 10, Legge 335/1995. INPS, circolare 2 marzo 2012, n. 31.	10 anni

I. APPENDICE: Violazioni

Riferimenti

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali 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.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Linee guida sulla notifica delle violazioni dei dati personali ai sensi del RGPD

Nel marzo 2023 lo "European Data Protection Board" ha adottato delle Linee Guida sulle violazioni dei dati personali che forniscono preziose informazioni su quando è necessario notificare la violazione alle autorità di controllo.

Per valutare la gravità di una violazione è necessario tenere conto del contesto nel quale si è verificata, dell'identificabilità dei dati violati e delle circostanze.

Contesto della violazione

Per valutare il contesto è necessario analizzare il tipo di dati violati (Dati semplici, comportamentali, finanziari, particolari, ecc.).

Fattori che aumentano i rischi sono:

- **Volume di dati per lo stesso interessato**: una sola informazione o tutto il fascicolo, un singolo acquisto o tutti gli acquisti del mese, ecc.
- **Caratteristiche del Titolare**: Potrebbero suggerire ipotesi su stato di salute (Ospedale, Farmacia) o opinioni (Partito, Chiesa), ecc.
- **Caratteristiche degli interessati**: Vulnerabili, Minori, ecc.

Fattori che possono portare ad una diminuzione della valutazione dei rischi:

- **Imprecisione dei dati**: dati non aggiornati, dati non verificati, ecc.
- **Disponibilità pubblica**: Eletti di un Partito, dati ricavabili facilmente dal WEB, ecc.
- **Natura dei dati**: Certificati di buona salute, Regolarità nei pagamenti, ecc.

Identificabilità dei dati violati

Per valutare i rischi è necessario analizzare quanto i dati violati permettono di identificare l'interessato.

Per i vari tipi di dati è opportuno effettuare specifiche valutazioni. Ad esempio:

- **Nome e Cognome**: Grado omonimia (Nazione, Regione, Città, Quartiere, Condominio).
- **Documento d'identità**: Solo il numero, contiene data di nascita (CF), con altre informazioni (indirizzo, e-mail, ecc.)
- **Numero Telefono / Indirizzo**: Già presenti in elenchi pubblici, in una Città, in una Nazione.
- **Indirizzo e-mail**: Senza riferimento al nome, non è l'indirizzo principale, viene utilizzato come identificativo per siti.
- **Immagine**: Poco chiara, con informazioni aggiuntive, con informazioni specifiche (appartenenza ad un gruppo, indirizzo di abitazione, ecc.).

Circostanze relative alla violazione

Se la violazione è a seguito di un evento malevolo è necessario supporre che i dati verranno utilizzati per danneggiare l'immagine del titolare o degli interessati.

Negli altri casi è necessario valutare:

Perdita di Riservatezza:

Possiamo considerare poco gravi alcuni tipi di violazioni quali, ad esempio:

- Smarrimento di un documento o di un portatile durante il trasporto.
- Smaltimento senza distruzione sicura.
- E-mail con dati personali inviata per errore ad un certo numero di destinatari noti.

Devono portare ad un incremento della valutazione del rischio violazioni tipo:

- Dati pubblicati su internet.
- Accesso a dati interni per errata configurazione di un sito web.

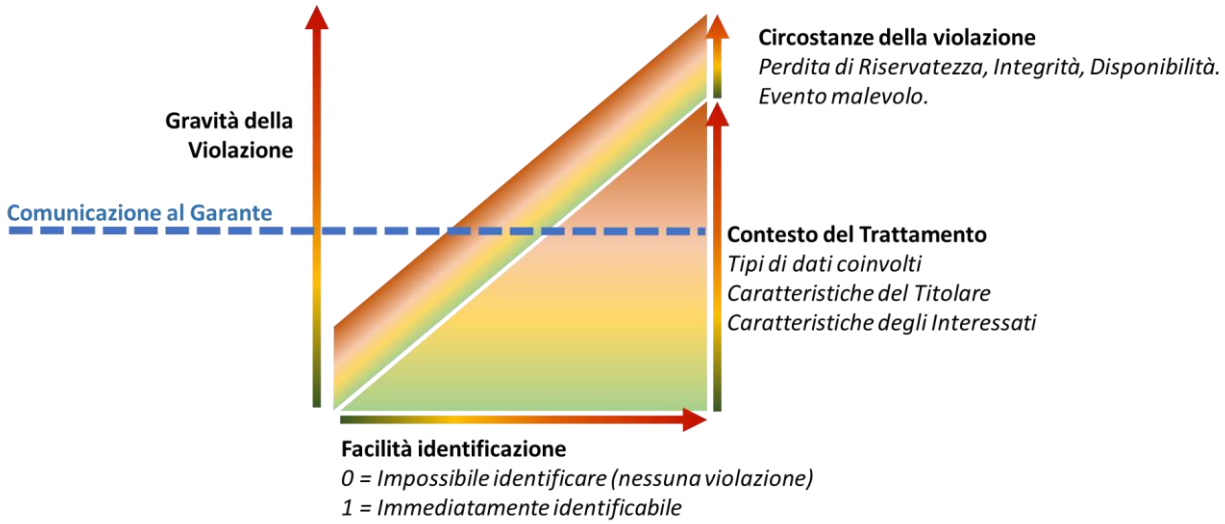
Perdita di integrità:

La violazione sarà meno grave se i dati sono alterati ma è possibile il recupero rispetto al caso in cui non vi sia la possibilità di recupero.

Perdita di disponibilità:

La gravità della violazione deve essere valutata, in caso di perdita dei dati, in relazione alle situazioni (di seguito situazioni via via più critiche):

- Sono disponibili copie di backup aggiornate.
- I dati sono recuperabili da altri a seguito di elaborazioni che richiedono un certo tempo.
- I dati devono essere richiesti agli interessati.
- Assenza di copie ed impossibilità di richiederli all'interessato.



J. APPENDICE: Diritti

Riferimenti

Articolo 15 - Diritto di accesso dell'interessato (C63, C64)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Articolo 16 - Diritto di rettifica (C65)

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») (C65, C66)

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 (C67)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un

diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

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

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

Articolo 20 - Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Articolo 21 - Diritto di opposizione

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

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

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

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Articolo 23 - Limitazioni

1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:

a) le finalità del trattamento o le categorie di trattamento;
b) le categorie di dati personali;
c) la portata delle limitazioni introdotte;
d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;
f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
g) i rischi per i diritti e le libertà degli interessati; e
h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

K. APPENDICE: Valutazione d'impatto sulla protezione dei dati

Riferimenti

Articolo 35 - Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una 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, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

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

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10.Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e),trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11.Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Allegato al provvedimento del Garante italiano dell'ottobre 2018

Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

- 1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".
- 2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
- 3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
- 4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
- 5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
- 6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
- 7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
- 8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

- 9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
- 10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
- 11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
- 12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività

Trattamenti da sottoporre a valutazione d'impatto

All'interno dello "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto" predisposto dal Garante italiano nell'Ottobre 2018 si ritiene possa essere di interesse delle imprese edili unicamente il punto 5:

"Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti."

In quanto, fra i punti previsti dal WP 248 presenta i criteri: 3-Monitoraggio sistematico; 7-Dati relativi a interessati vulnerabili; 8-Applicazione di nuove soluzioni tecnologiche.

In base all'Art. 35 del RGPD la valutazione deve contenere almeno:

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento.
- Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità.
- Una valutazione dei rischi per i diritti e le libertà degli interessati.
- Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Si ritiene che le specifiche valutazioni d'impatto (DPIA) predisposte nelle modalità sopra esposte ed il riferimento ai provvedimenti del Garante (in materia di videosorveglianza del 8 aprile 2010 e sui Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro del 4 ottobre 2011) possano essere considerate valutazioni adeguate ai sensi dell'Art. 35 del RGPD.