La protezione dei dati personali nella gestione delle imprese ricettive

la privacy nell'ospitalità

Federica Bonafaccia

con il contributo di

ENTE BILATERALE NAZIONALE TURISMO

FEDERALBERGHI
Federazione delle Associazioni Italiane Alberghi e Turismo

FEDERALBERGHI

LA PROTEZIONE DEI DATI PERSONALI
NELLA GESTIONE DELLE IMPRESE RICETTIVE

la privacy nell'ospitalità

quarta edizione

La protezione dei dati personali nella gestione delle imprese ricettive

(la privacy nell'ospitalità)

di Federica Bonafaccia

Si ringrazia l'Ente Bilaterale Nazionale del settore Turismo per il contributo alla realizzazione della quarta edizione.

EDIZIONI ISTA
Istituto Internazionale di Studi
e Documentazione Turistico Alberghiera
"Giovanni Colombo"
00187 Roma – via Toscana 1

INDICE

1. IL QUADRO NORMATIVO

A decorrere dallo scorso 25 maggio 2018, il Regolamento (UE) 2016/679 “General Data Protection Regulation” (GDPR) in materia di protezione dei dati personali è obbligatorio in tutti i suoi elementi nonché direttamente applicabile in ciascuno degli Stati membri.

Al fine di armonizzare la normativa italiana, di cui al Codice della privacy (decreto legislativo n. 196 del 2003), con le disposizioni del Regolamento europeo, è stato emanato il decreto legislativo n. 101 del 10 agosto 2018, con il quale sono state abrogate le disposizioni del Codice incompatibili con le disposizioni contenute nel Regolamento europeo.

Premesso che l’obiettivo di tutela dei diritti e delle libertà fondamentali della persona va ora perseguito prioritariamente secondo le prescrizioni del regolamento europeo, il Codice della privacy rimane in vigore anche se privato delle sue prescrizioni fondamentali.

1.1 ambito di applicazione

Il Regolamento (UE) 2016/679 “General Data Protection Regulation” (GDPR) si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (articolo 2).

Non sono ricompresi nel campo di applicazione del Regolamento i trattamenti relativi ai dati che riguardano le persone giuridiche, gli enti e le associazioni. La tutela rimane pertanto assicurata solo per i dati che riguardano le persone fisiche.

Il Regolamento non si applica ai trattamenti di dati personali effettuati da una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico, e quindi senza una connessione con un’attività commerciale o professionale. Da ciò si deduce che le prescrizioni del Regolamento devono essere rispettate anche dai soggetti che esercitano attività ricettiva occasionalmente, e quindi senza partita IVA, per i trattamenti svolti nell’ambito di tale attività.

Rientrano formalmente nel campo di applicazione della normativa i trattamenti di dati personali di imprenditori individuali, società di persone o liberi professionisti, in quanto non sono “persone giuridiche”. Si tratta comunque di soggetti che, agendo come professionisti, necessitano sicuramente di minore protezione.

1.2 definizioni

Per comprendere la normativa ed il suo campo di applicazione, è indispensabile analizzare alcune definizioni tra quelle riportate nell’articolo 4 del Regolamento:

- *“dato personale”:* qualsiasi informazione riguardante una persona fisica identificata o identificabile *(“interessato”);*
- *“trattamento”:* qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a

disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- *"limitazione di trattamento":* il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- *"profilazione":* qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- *"pseudonimizzazione"*: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- *"archivio":* qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- *"titolare del trattamento":* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- *"responsabile del trattamento":* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- *"destinatario"*: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
- *"terzo"*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- *"consenso dell'interessato"*: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento;
- *"rappresentante":* la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta.

1.3 principio di liceità

Secondo il principio di liceità (articolo 5), i dati personali devono essere:

- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno.

1.4 base giuridica

Ogni trattamento deve trovare fondamento in un'idonea base giuridica (articolo 6). Il trattamento è lecito solo se, e nella misura in cui, ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il **consenso al trattamento dei propri dati personali** per una o più specifiche finalità;
- 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;
- il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- 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;
- il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**, prevalente rispetto al diritto di protezione dei dati dell'interessato.

1.5 consenso

Qualora il trattamento sia basato sul consenso (ad esempio nei casi in cui il titolare non ha il diritto o l'obbligo legale di trattare i dati, o il trattamento non è effettuato in esecuzione di un contratto o in adempimento di misure precontrattuali), questo deve essere informato, specifico, libero ed inequivocabile (articolo 7).

Per quanto riguarda i minori, il novellato Codice della privacy (articolo 2 quinquies), in attuazione del Regolamento europeo, fissa a 14 anni l'età valida per l'espressione del consenso in relazione all'offerta diretta di servizi della società dell'informazione (iscrizione a social network, servizi di messaggistica, eccetera). Per i soggetti di età inferiore a 14 anni il consenso è espresso da chi esercita la responsabilità genitoriale. Al di fuori di tali servizi, resta il limite dei 18 anni per la prestazione di un valido consenso al trattamento dei dati.

Non è richiesta la forma scritta, né che sia "documentato per iscritto", ma il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

1.6 categorie particolari di dati personali

Tranne nei casi sotto indicati, 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 (cosiddetti "dati sensibili" - articolo 9).

Il divieto, con alcune garanzie previste dal diritto nazionale, non si applica in alcuni specifici casi, tra cui:

- se l'interessato ha prestato il proprio **consenso**, che deve essere esplicito, al trattamento di tali dati personali per una o più finalità specifiche;
- se 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;
- se 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;
- se 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;
- se il trattamento riguarda **dati personali resi manifestamente pubblici dall'interessato**, o è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, o è necessario per motivi di interesse pubblico;
- se 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**.

Il Regolamento prevede che gli Stati membri possano mantenere o introdurre ulteriori condizioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. Al riguardo, il decreto legislativo n. 101 del 2018 delega il Garante per la protezione dei dati personali a prescrivere misure di garanzia adottando uno specifico provvedimento, previa consultazione pubblica, con cadenza almeno biennale. Le misure di garanzia potranno individuare ulteriori condizioni di liceità del trattamento, in particolare specifiche prescrizioni di sicurezza, comprese le tecniche di cifratura e pseudonomizzazione, e l'accesso selettivo. Rimane fermo il divieto di diffondere dati genetici, biometrici o relativi alla salute (articolo 2 septies Codice privacy). Nelle more dell'emanazione di tale provvedimento, rimangono in vigore in via transitoria le misure di garanzia previste dalle

autorizzazioni generali già emanate dal Garante ai sensi dell'articolo 40 del previgente Codice della privacy.

1.7 informativa

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (articoli 12, 13 e 14). Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (articolo 12, paragrafo 7). Queste icone dovranno essere identiche in tutta l'UE e saranno definite dalla Commissione europea.

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento.

Nel caso di dati personali non raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato).

Tra le informazioni che il titolare del trattamento deve obbligatoriamente fornire all'interessato:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati (DPO), ove applicabile;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari;
- se trasferisce i dati personali in Paesi terzi.

In aggiunta, 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:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza di diritti per l'interessato (diritto di accesso, rettifica, cancellazione, limitazione, opposizione) e la possibilità di proporre reclamo all'autorità di controllo;
- 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;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione;

- qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento indica all'interessato la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Relativamente **all'obbligo di indicare nell'informativa i destinatari dei dati personali dell'interessato**, ricordiamo che l'articolo 4 del Regolamento, al punto 9), definisce **"destinatario" la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi**. Si specifica inoltre che **le autorità pubbliche a cui i dati personali sono comunicati, conformemente a un obbligo legale ai fini dell'esercizio della loro missione istituzionale, non sono considerate "destinatari"** (considerando n. 31). Il Regolamento non definisce però cosa si intende per "comunicazione".

A fini di chiarezza terminologica, il decreto legislativo n. 101 del 2018 introduce specifiche definizioni di "comunicazione" e "diffusione" di dati personali, non presenti nel Regolamento europeo.

Si intende per "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione. Si intende per "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. (articolo 2 ter, comma 4, del novellato Codice privacy).

Pertanto, continueranno a non essere considerati "destinatari", ad esempio, i consulenti che effettuano adempimenti di tipo fiscale o connessi con i rapporti di lavoro, se nominati responsabili o in alternativa se autorizzati al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (i soggetti che il previgente Codice della privacy definiva "incaricati").

1.8 diritti dell'interessato

All'interessato sono riconosciuti alcuni diritti, riportati negli articoli da 15 a 22 del Regolamento. Nel caso in cui l'interessato richieda di far valere un proprio diritto, il titolare del trattamento deve fornire riscontro entro un mese dalla richiesta, termine prorogabile di due mesi in casi di particolare complessità (articolo 12, comma 3).

Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo all'autorità di controllo (Garante della protezione dei dati) e di proporre ricorso giurisdizionale (articolo 12, comma 4).

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

- addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

- rifiutare di soddisfare la richiesta. In questo caso ha l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta (articolo 12, comma 5).

Di seguito, la sintesi dei diritti spettanti all'interessato.

Diritto di accesso - 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 caso affermativo, ottenere informazioni sulle finalità e modalità del trattamento (articolo 15). 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.

Diritto di rettifica - L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo (articolo 16).

Diritto alla cancellazione (diritto all'oblio) - L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali (articolo 17) che lo riguardano senza ingiustificato ritardo se la conservazione di tali dati viola i principi del Regolamento o di altra norma italiana o dell'Unione. In particolare, l'interessato ha il diritto di chiedere che siano cancellati i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

Diritto di limitazione di trattamento - L'interessato ha, in alcune ipotesi, il diritto di ottenere la limitazione del trattamento, ad esempio quando l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali (articolo 18). Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

Diritto alla portabilità dei dati - 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, qualora il trattamento si basi sul consenso o è effettuato in esecuzione di un contratto o di misure precontrattuali, e sia automatizzato (articolo 20).

Diritto di opposizione - L'interessato ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, o effettuato per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, compresa la profilazione (articolo 21). Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che 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. 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.

Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione - 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 (articolo 22). il titolare del trattamento deve attuare in alcuni casi 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.

1.9 valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza

Nell'ambito del principio di "responsabilizzazione" (accountability), il Regolamento prevede che venga rispettato il criterio sintetizzato dall'espressione inglese "data protection by default and by design". Secondo tale principio, prima di avviare iniziative che comportano il trattamento di dati personali, occorre prevedere e configurare le garanzie indispensabili per conformarsi al Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio, con un'analisi preventiva che deve poi sostanziarsi in una serie di attività specifiche e dimostrabili.

Il titolare analizza quindi i rischi inerenti il trattamento, quali la distruzione, la perdita, la modifica, la rivelazione o l'accesso non autorizzato, che potrebbero cagionare un danno fisico, materiale o immateriale (articoli 24, 25, 28, 29, 32, 40, 41, 42 e 43). A seguito dell'analisi dei rischi, viene valutato l'adeguato livello di sicurezza, attuando le misure ritenute idonee per limitare tali rischi.

Il titolare del trattamento deve quindi mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento europeo, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Dette misure sono riesaminate e aggiornate qualora necessario.

Le misure tecniche e organizzative comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative.

Dopo l'entrata in vigore del Regolamento, pertanto, non potranno più sussistere obblighi generalizzati di adozione di "misure minime di sicurezza" (quali quelle finora previste dal disciplinare di cui all'allegato B del previgente Codice della privacy), poiché tale

valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati. L'Autorità Garante valuterà se approvare linee guida o definire buone prassi. **L'Autorità ritiene comunque che le prescrizioni di cui all'allegato B al previgente Codice privacy abbiano fatto conseguire in questi anni risultati positivi in termini di sicurezza e protezione dei dati. Per i trattamenti effettuati in adempimento di un obbligo legale, l'Autorità ritiene che potranno restare in vigore le misure di sicurezza di cui all'allegato B del previgente Codice della privacy.**

Per quanto riguarda le misure organizzative, il Regolamento richiede che il responsabile del trattamento, definito come la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento, ove nominato dal titolare, debba presentare garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Il responsabile del trattamento, o chiunque agisce sotto la sua autorità o sotto quella del titolare del trattamento, non può trattare dati personali se non è istruito in tal senso dal titolare del trattamento. **È necessario pertanto che i soggetti incaricati dal titolare o dal responsabile di effettuare un trattamento, o singole fasi di esso, ricevano specifiche istruzioni da seguire.**

1.10 valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment)

Quando il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità, **deve essere svolta una valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment)** (articolo 35).

Il Regolamento definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi e dimostrare la conformità al Regolamento.

All'esito della valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'Autorità Garante per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

L'articolo 35, paragrafo 4, del Regolamento europeo rimette alle autorità di controllo nazionali il compito di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto, e di comunicarlo al Comitato europeo per la protezione dei dati (organo composto dalle autorità nazionali di controllo).

Il Comitato europeo per la protezione dei dati, in data 25 maggio 2018, facendo proprie le linee guida elaborate dal Gruppo di Lavoro "Articolo 29" (WP 248, rev. 01), ha

individuato i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato":

1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "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) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone;
3) monitoraggio sistematico degli interessati;
4) dati sensibili o dati aventi carattere altamente personale;
5) trattamento di dati su larga scala;
6) creazione di corrispondenze o combinazione di insiemi di dati;
7) dati relativi a interessati vulnerabili;
8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
9) quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Il ricorrere di due o più dei predetti criteri è considerato come indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è quindi richiesta una valutazione d'impatto sulla protezione dei dati.

Tenendo conto di tali criteri, il Garante ha predisposto un elenco delle tipologie di trattamento da sottoporre a valutazione preventiva d'impatto[1]. L'elenco non è esaustivo, restando fermo quindi l'obbligo di adottare una valutazione d'impatto nel caso ricorrano due o più dei criteri sopra elencati. Inoltre, resta ferma la facoltà del titolare del trattamento di assoggettare a valutazione d'impatto un trattamento che presenti solo uno dei predetti criteri.

Di seguito, la descrizione dei trattamenti per i quali è richiesta la 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

[1] Provvedimento del Garante n. 467 dell'11 ottobre 2018 (doc. web n. 9058979)

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 di trattamento.

L'elenco potrà essere ulteriormente modificato o integrato anche sulla base delle risultanze emerse nel corso della prima fase di applicazione del GDPR.

Per aiutare le aziende, soprattutto quelle di piccola dimensione, a conformarsi alle prescrizioni del Regolamento europeo, la CNIL, autorità francese per la protezione dei dati, ha messo a disposizione sul proprio sito un software[2], scaricabile gratuitamente, di ausilio in vista della effettuazione della valutazione d'impatto sulla protezione dei dati.

[2] Una volta aperta la pagina https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil, scorrere fino al titolo "Version portable" e selezionare il tipo di sistema operativo installato sul proprio computer. Una volta scaricato il software, lanciare l'installazione che sarà effettuata automaticamente nella versione in lingua italiana.

Il software offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal Gruppo di lavoro “Articolo 29” nelle Linee-guida sulla DPIA. La versione in lingua italiana è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali.

1.11 codici di condotta

Il titolare del trattamento può utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Viene infatti incoraggiata l’elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentativi di categorie di soggetti titolari o responsabili di trattamenti possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l’applicazione del Regolamento. Il codice di condotta deve essere approvato dall’Autorità Garante.

Il controllo della conformità con un codice di condotta può essere effettuato da un organismo di certificazione accreditato.

1.12 designazione del responsabile della protezione dei dati - DPO

Il titolare o il responsabile del trattamento designano un responsabile della protezione dei dati (DPO - Data Protection Officer, articolo 37) ogniqualvolta:

- le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

  oppure

- le attività principali del titolare o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali (dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché 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), o i dati personali relativi a condanne penali e a reati.

Dalla lettura delle considerazioni preliminari del Regolamento (considerando n. 97) si evince che l’obbligo di designazione del DPO sussiste solo se il trattamento di dati costituisce l’attività primaria, e non si tratta di attività accessoria.

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti assegnati dal Regolamento, tra cui informare e fornire consulenza in materia di protezione dei dati al titolare o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento.

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

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

L'Autorità Garante ha chiarito che la normativa attuale non prevede l'obbligo per i candidati a DPO di possedere attestati formali delle competenze professionali. Tali attestati, rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una "abilitazione" allo svolgimento del ruolo di DPO. La normativa attuale, tra l'altro, non prevede l'istituzione di un albo dei "responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto. I soggetti tenuti alla nomina del DPO dovranno quindi procedere alla sua selezione valutando autonomamente il possesso dei requisiti necessari per svolgere i compiti da assegnare.

Ricorrendo i presupposti di cui sopra (monitoraggio regolare e sistematico degli interessati su larga scala), secondo l'Autorità Garante sono tenuti alla nomina del DPO, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; **sindacati**; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, **terme**, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

Per il Garante, la designazione del DPO non è obbligatoria, ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

Pertanto, **nella generalità dei casi le aziende alberghiere, se ed in quanto non effettuano trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, non sono obbligate alla nomina del DPO.**

In ogni caso, il Garante, anche alla luce del principio di "accountability" che permea il Regolamento, raccomanda comunque la designazione di tale figura. Nel caso in cui si ritenga di nominare un DPO, occorre rispettare le prescrizioni del Regolamento europeo e le indicazioni fornite dal Garante.

1.13 registro delle attività di trattamento

Il titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro deve contenere tutte le informazioni sui trattamenti effettuati, elencate nell'articolo 30 del Regolamento.

La tenuta del registro non è obbligatoria per le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano presenti un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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), **o dati personali relativi a condanne penali e a reati**.

Il Garante per la protezione dei dati personali ha pubblicato sul proprio sito le istruzioni sulla compilazione del registro delle attività di trattamento, chiarendo gli aspetti relativi ai soggetti obbligati alla sua compilazione.

Il registro, che deve essere predisposto dal titolare e dal responsabile del trattamento, è un documento contenente le principali informazioni (specificatamente individuate dall'articolo 30 del Regolamento) relative alle operazioni di trattamento svolte da imprese, associazioni o professionisti.

Secondo il Garante, la tenuta del registro dei trattamenti non costituisce un adempimento formale, ma è bensì parte integrante di un sistema di corretta gestione dei dati personali. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda.

L'obbligo di redigere il registro costituisce uno dei principali elementi di accountability del titolare, poiché rappresenta uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile ai fini della valutazione o analisi del rischio e dunque preliminare rispetto a tale attività.

Dalla lettura delle FAQ rese disponibili dal Garante, emerge una interpretazione estensiva dell'obbligo di redigere il registro rispetto alle non chiare indicazioni del Regolamento europeo. Secondo il Garante, in ambito privato, i soggetti obbligati alla tenuta del registro sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9 paragrafo 1 GDPR (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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), o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR.

Alla luce di quanto sopra, il Garante ritiene che siano tenuti all'obbligo di redazione del registro, ad esempio:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);

- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (per esempio, organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti eccetera; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso eccetera; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (ad esempio, delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Il Garante precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (ad esempio, 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).

Al di fuori dei casi di tenuta obbligatoria del registro, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare e in quello del responsabile.

Finalità del trattamento: la finalità va indicata per ciascuna tipologia di trattamento (ad esempio, trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini). Il Garante ritiene opportuno indicare anche la base giuridica del trattamento;

Descrizione delle categorie di interessati e delle categorie di dati personali: andranno specificate sia le tipologie di interessati (ad esempio, clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (ad esempio dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, eccetera);

Categorie di destinatari a cui i dati sono stati o saranno comunicati: andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (ad esempio, enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, il Garante ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (ad esempio, soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale: andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente

all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del GDPR (ad esempio, decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, eccetera);

Termini ultimi previsti per la cancellazione delle diverse categorie di dati: dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad esempio, "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (ad esempio, norme di legge, prassi settoriali) indicativi degli stessi (ad esempio, "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");

Descrizione generale delle misure di sicurezza: andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'articolo 32 del GDPR tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B alla previgente versione del Codice della privacy) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (ad esempio, procedure organizzative interne; security policy eccetera).

Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ad esempio le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento eccetera.).

Il registro dei trattamenti **deve essere mantenuto costantemente aggiornato** poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel registro, dando conto delle modifiche sopravvenute.

Il registro **può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento**. In quest'ultimo caso il registro dovrà recare una annotazione del tipo:

"- scheda creata in data XY"

"- ultimo aggiornamento avvenuto in data XY".

Il responsabile del trattamento tiene un registro di "tutte le categorie di attività relative al trattamento svolte per conto di un titolare" (art. 30, paragrafo 2 del GDPR).

In merito alle modalità di compilazione, il Garante rappresenta quanto segue:

- nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (ad esempio società di software house), le informazioni dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari. Il responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce; nel caso in cui il responsabile

operi per un elevato numero di titolari, e l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad esempio, a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dal Regolamento europeo;

- con riferimento alla "descrizione delle categorie di trattamenti effettuati", è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'articolo 28 del GDPR, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo;
- in caso di sub-responsabile, il registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'articolo 28, paragrafi 2 e 4 del GDPR.

L'Autorità Garante ha messo a disposizione dei titolari e responsabili di trattamenti un modello di registro, realizzato per le piccole e medie imprese che dovrà essere compilato e integrato nei modi opportuni. Abbiamo provveduto a implementare il modello reso disponibile dal Garante con alcune informazioni, a mero titolo esemplificativo, utili per aiutare le imprese ricettive nella sua compilazione[3].

1.14 notifica delle violazioni di dati personali

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'Autorità Garante 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 (**data breach** - articoli 33 e 34). Qualora la notifica al Garante non sia effettuata entro 72 ore, deve essere corredata dei motivi del ritardo.

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.

1.15 diritto al risarcimento e responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione di una norma del Regolamento ha il diritto di ottenere il risarcimento dal titolare o dal responsabile del trattamento, a meno che l'evento dannoso non sia loro imputabile (articolo 82).

[3] Vedi il modello di registro nel capitolo "i modelli" al punto 4.11.

1.16 sanzioni amministrative pecuniarie e sanzioni penali

Ai sensi del Regolamento europeo, l'autorità nazionale (Autorità Garante) provvede affinché le sanzioni amministrative pecuniarie ivi previste siano in ogni singolo caso effettive, proporzionate e dissuasive (articoli 83 e 84).

Nei casi più gravi, il Regolamento prevede sanzioni amministrative pecuniarie fino a 20 milioni di euro, o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Con l'obiettivo di mitigare la mancanza di sanzioni edittali nel minimo, il decreto legislativo n. 101 del 2018 **introduce una forma di oblazione** consistente nella possibilità per il trasgressore, entro 30 giorni (60 in caso di residenza all'estero) dalla data di comunicazione del provvedimento di irrogazione della sanzione, di definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e **mediante il pagamento di un importo pari alla metà della sanzione irrogata** (articolo 166, comma 8, del novellato Codice privacy).

Al Garante della protezione dei dati vengono attribuiti i poteri di controllo, di diffida e di adozione delle sanzioni amministrative, esercitabili attraverso procedimenti da definire con specifico regolamento (articolo 166, comma 9, del novellato Codice privacy).

Per i primi 8 mesi decorrenti dalla data di entrata in vigore del decreto legislativo n. 101 del 2018, cioè fino al 19 maggio 2019, il Garante tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento europeo, della fase di prima applicazione delle disposizioni sanzionatorie. Non si tratta quindi di una moratoria, ma della aggiunta di un'ulteriore condizione di cui il Garante dovrà tenere conto in sede di applicazione delle sanzioni amministrative, che, secondo il disposto dell'articolo 83 del Regolamento europeo, dovranno essere "in ogni singolo caso effettive, proporzionate e dissuasive".

Alcune sanzioni penali previste nel testo precedente del Codice della privacy sono abrogate e sostituite dalle ingenti sanzioni amministrative di cui all'articolo 83 del Regolamento europeo. Sono state però introdotte nuove fattispecie di reato per i comportamenti che, per vastità di dimensione, coinvolgono un numero rilevante di persone offese, e nelle ipotesi di false comunicazioni al Garante.

2. AUTORIZZAZIONI E LINEE GUIDA DEL GARANTE

Il decreto legislativo n. 101 del 2018 ha stabilito che continuano a produrre effetti i provvedimenti del Garante emanati prima del 25 maggio 2018, compatibili con i principi contenuti nel Regolamento europeo.

In attesa di chiarimenti da parte del Garante sulla valutazione di compatibilità con il Regolamento europeo, sintetizziamo di seguito il contenuto di alcuni provvedimenti di maggiore interesse, che, benché precedenti l'entrata in vigore del Regolamento, sembrano conformi ai suoi principi.

2.1 la gestione del rapporto di lavoro

Allo scopo di fornire indicazioni e raccomandazioni ai datori di lavoro del settore privato sulle operazioni di trattamento di dati personali, anche "particolari" (ex sensibili), dei lavoratori, il Garante ha a suo tempo emanato alcune specifiche linee guida[4].

Nell'ambito dei rapporti di lavoro, i trattamenti effettuati dal datore di lavoro riguardano normalmente i **dati anagrafici dei lavoratori**, nonché altre informazioni connesse allo svolgimento dell'attività lavorativa (la tipologia del contratto, la qualifica, la retribuzione, il tempo di lavoro anche straordinario, ferie e permessi, assenza dal servizio, procedimenti disciplinari, eccetera). È possibile che vengano trattatati dati biometrici e dati particolari, riferiti anche a terzi (credo religioso, adesione a sindacati, dati che rivelano lo stato di salute contenuti in certificati medici o in altra documentazione).

I dati personali del lavoratore possono essere trattati dal datore di lavoro nella misura in cui **ciò sia necessario per dare corretta esecuzione al rapporto di lavoro**. Le informazioni trattate devono essere pertinenti e non eccedenti le finalità perseguite, e devono essere osservate tutte le disposizioni della normativa italiana ed europea, fra cui:

- rispetto dei principi di necessità e liceità;
- obbligo di fornire ai dipendenti un'adeguata informativa;
- richiesta preventiva del consenso nei casi in cui il Regolamento europeo lo prevede (quando il trattamento non 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, e non sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri);
- rispetto delle prescrizioni impartite dal Garante, anche nelle autorizzazioni di carattere generale per il trattamento di dati particolari o relativi a condanne penali e reati (autorizzazione generale n. 1/2016[5], valida fino al 24 maggio 2018, la cui validità è stata prorogata dal decreto legislativo n. 101 del 2018);
- adozione delle misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi ed utilizzazioni indebite, rispetto ai quali il datore di lavoro può essere chiamato a rispondere civilmente e penalmente.

Le linee guida richiamano l'attenzione sulla necessità di identificare le figure soggettive che, a diverso titolo, possono trattare i dati, definendo chiaramente le rispettive

[4] Provvedimento n. 53 del 23 novembre 2006, GU n. 285 del 7.12.2006 - doc. web n. 1364939.

[5] Autorizzazione n. 1/2016 - Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro - 15 dicembre 2016- doc. web n. 5800451.

attribuzioni. Nelle realtà imprenditoriali più articolate l'identificazione spesso non risulta agevole, ostacolando l'esercizio dei diritti dei lavoratori.

Tra queste figure, si segnala **il medico competente**, che è legittimato a istituire, curandone l'aggiornamento, una **cartella sanitaria e di rischio** a seguito di accertamenti preventivi e periodici sui lavoratori. Detta cartella è **custodita presso l'azienda**, con salvaguardia del segreto professionale, e consegnata in copia al lavoratore al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne faccia richiesta. Il medico competente è quindi deputato a trattare i dati sanitari dei lavoratori, procedendo alle dovute annotazioni nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate. **Alle predette cartelle il datore di lavoro non può accedere**, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali aziendali (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti) con salvaguardia del segreto professionale. Il datore di lavoro è tenuto ad adottare le misure preventive e protettive per i lavoratori, su parere del medico competente o qualora il medico lo informi di anomalie imputabili all'esposizione a rischio, ma non può conoscere le eventuali patologie accertate, ma solo la valutazione finale circa l'idoneità del dipendente, dal punto di vista sanitario, allo svolgimento di date mansioni.

L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta, partendo dal modello di riferimento, e la sua ulteriore "utilizzazione" a loro insaputa. **L'utilizzo di dati biometrici può essere giustificato solo in casi particolar**i, per presidiare accessi ad "aree sensibili" (processi produttivi pericolosi o sottoposti a segreti di varia natura, o per locali destinati alla custodia di beni o documenti segreti o riservati o di valore). Inoltre, nei casi in cui l'uso dei dati biometrici è consentito, i sistemi informativi devono essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali, e da escluderne il trattamento quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità. **Per fattispecie particolari o in ragione di situazioni eccezionali, il Regolamento europeo prevede l'obbligo di effettuare la valutazione preventiva di impatto (DPIA) sottoponendo eventualmente la questione al Garante.**

Il datore di lavoro, **qualora non ricorrano le condizioni di legittimazione previste dal Regolamento europeo, deve chiedere il consenso al lavoratore per comunicare i suoi dati a terzi** (ad esempio, ad associazioni di datori di lavoro o di ex dipendenti; a conoscenti, familiari e parenti).

Ai sensi del provvedimento del Garante, **non costituisce comunicazione a terzi la conoscenza dei dati da parte dei soggetti, interni o esterni, incaricati del trattamento da parte del datore di lavoro**. Infatti, il datore di lavoro ha piena facoltà di disciplinare le modalità del trattamento, designando i soggetti, interni o esterni, incaricati o responsabili del trattamento, che possono acquisire conoscenza dei dati inerenti alla gestione del rapporto di lavoro, in relazione alle funzioni svolte e a idonee istruzioni scritte alle quali attenersi.

Il datore di lavoro può comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o gruppi di lavoratori.

Il consenso del lavoratore è necessario per pubblicare sue informazioni personali (fotografia, informazioni anagrafiche o curriculum) nella intranet aziendale (e a maggior ragione in Internet), non risultando tale ampia circolazione di dati personali di regola necessaria per eseguire obblighi derivanti dal contratto di lavoro.

In assenza di consenso, o di specifiche disposizioni normative che la impongano o autorizzino, la diffusione di dati personali riferiti ai lavoratori può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro (affissione nella bacheca aziendale di ordini di servizio, di turni lavorativi o feriali, di disposizioni riguardanti l'organizzazione del lavoro e l'individuazione delle mansioni cui sono deputati i singoli dipendenti). Non è invece di regola lecito dare diffusione a informazioni personali di singoli lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi, come ad esempio:

- affissione relativa ad emolumenti percepiti o che fanno riferimento a particolari condizioni personali;
- sanzioni disciplinari irrogate o informazioni relative a controversie giudiziarie;
- assenze dal lavoro per malattia;
- iscrizione e/o adesione dei singoli lavoratori ad associazioni.

Costituisce diffusione di dati personali riportare ed esibire informazioni personali su cartellini identificativi appuntati ad esempio sull'abito o sulla divisa del lavoratore (di solito, con lo scopo di migliorare il rapporto fra operatori ed utenti o clienti). Al riguardo, il Garante ha già rilevato che **l'obbligo di portare in modo visibile un cartellino identificativo può trovare fondamento in alcune prescrizioni contenute in accordi sindacali aziendali, il cui rispetto può essere ricondotto alle prescrizioni del contratto di lavoro**. Tuttavia, in relazione al rapporto con il pubblico, si è ravvisata la sproporzione dell'indicazione sul cartellino di dati personali identificativi (generalità o dati anagrafici), **ben potendo spesso risultare sufficienti altre informazioni (quali codici identificativi, il solo nome o il ruolo professionale svolto)**, per sé sole in grado di essere d'ausilio all'utenza.

Il datore di lavoro deve adottare cautele nelle forme di comunicazione con il lavoratore, adottando le misure più opportune per **prevenire un'indebita conoscenza di dati personali del lavoratore da parte di terzi** (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

Il datore di lavoro **deve osservare cautele particolari nel trattamento dei dati particolari dei lavoratori, quali ad esempio quelli idonei a rivelarne lo stato di salute**. Costituisce dato particolare idoneo a rivelare lo stato di salute del lavoratore l'informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla contestuale enunciazione della diagnosi. Per tali informazioni, oltre alla normativa sulla privacy, anche lo Statuto dei lavoratori richiede particolari accorgimenti per contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza per dare esecuzione al contratto.

La normativa sul lavoro ed i contratti collettivi giustificano il trattamento dei dati relativi ai casi di infermità che determinano un'incapacità lavorativa, temporanea o definitiva, con la conseguente sospensione o risoluzione del contratto. Il datore di lavoro può inoltre trattare dati relativi a invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia. A tale riguardo, infatti, sussiste un quadro normativo articolato che prevede anche l’obbligo del lavoratore di comunicare, e successivamente certificare, al datore di lavoro e all'ente previdenziale lo stato di malattia: obblighi funzionali non solo a giustificare i trattamenti normativi ed economici spettanti al lavoratore, ma anche a consentire al datore di lavoro, nelle forme di legge, di verificare le reali condizioni di salute del lavoratore.

Per attuare tali obblighi viene utilizzata un'apposita modulistica, consistente in un attestato di malattia da consegnare al datore di lavoro (con la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. "prognosi") e in un certificato di diagnosi da consegnare, a cura del lavoratore stesso, all'INPS o alla struttura pubblica indicata dallo stesso Istituto d'intesa con la regione, se il lavoratore ha diritto a ricevere l'indennità di malattia a carico dell'ente previdenziale.

Tuttavia**, qualora dovessero essere presentati dai lavoratori certificati medici con i dati di prognosi e di diagnosi, i datori di lavoro restano obbligati, ove possibile, ad adottare idonee misure e accorgimenti volti a prevenirne la ricezione o, in ogni caso, ad oscurare i dati di diagnosi.**

In alcuni casi il datore di lavoro può venire a conoscenza delle condizioni di salute del lavoratore. Nel caso di infortuni o malattie professionali dei lavoratori, ad esempio, la normativa prevede che la denuncia debba essere corredata da specifica certificazione medica. In tal caso, pur essendo legittima la conoscenza della diagnosi, il datore di lavoro deve limitarsi a comunicare all'ente assistenziale esclusivamente le informazioni sanitarie relative o collegate alla patologia denunciata, e non anche dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro.

Il datore di lavoro può trattare i dati relativi allo stato di salute del lavoratore, o di suoi congiunti (ad esempio informazioni relative a condizioni di disabilità) anche quando ciò è necessario per permettere al lavoratore di godere dei benefici di legge (come ad esempio permessi o periodi prolungati di aspettativa con conservazione del posto di lavoro). Il datore di lavoro può anche venire a conoscenza dello stato di tossicodipendenza del dipendente, che richieda di accedere a programmi riabilitativi o terapeutici con conservazione del posto di lavoro.

Il datore di lavoro è legittimato a comunicare i dati idonei a rivelare lo stato di salute dei lavoratori ai soggetti pubblici (enti previdenziali e assistenziali) tenuti a erogare le prescritte indennità, in adempimento a specifici obblighi derivanti dalla legge, da altre norme o regolamenti o da previsioni contrattuali, nei limiti delle sole informazioni indispensabili.

Il datore di lavoro è tenuto a rendere al lavoratore, prima di procedere al trattamento dei dati personali che lo riguardano (anche in relazione alle ipotesi nelle quali la legge non richieda il suo consenso), un'informativa individualizzata completa degli elementi indicati dal Regolamento europeo.

Il datore di lavoro deve adottare **idonee misure di sicurezza** a protezione dei dati personali dei dipendenti, con particolare attenzione per quelli “particolari”. Le informazioni contenenti dati particolari devono essere conservate separatamente da ogni altro dato personale dell'interessato, in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative.

Resta fermo l'obbligo del datore di lavoro di preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento, che deve avere cognizioni in materia di protezione dei dati personali e ricevere una formazione adeguata. Secondo il Garante, in assenza di un'adeguata formazione degli addetti al trattamento dei dati personali, il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito.

Il datore di lavoro deve adottare misure organizzative e fisiche idonee a garantire:

- che i luoghi ove si svolge il trattamento dei dati siano protetti da indebite intrusioni;
- che sia evitata l'indebita presa di conoscenza dei dati da parte di terzi;

- che siano impartite istruzioni agli incaricati in ordine alla osservanza del segreto d'ufficio;
- che sia impedita l'acquisizione e riproduzione di dati personali trattati elettronicamente da parte di soggetti non autorizzati, in assenza di adeguati sistemi di autenticazione o autorizzazione;
- che sia impedita l'involontaria acquisizione di informazioni personali da parte di terzi o di altri dipendenti: ad esempio adottando opportuni accorgimenti per il rispetto di distanze di sicurezza o per la trattazione di informazioni riservate in spazi chiusi.

I lavoratori possono esercitare nei confronti del datore di lavoro i diritti previsti dal Regolamento (articolo da 15 a 22).

Il datore di lavoro è tenuto a fornire un riscontro completo alla richiesta del lavoratore, comunicando in modo chiaro e intelligibile tutte le informazioni in suo possesso.

Nel fornire riscontro, il titolare del trattamento deve comunicare i dati richiesti ed effettivamente detenuti, e non è tenuto a ricercare o raccogliere altri dati che non siano nella propria disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento.

2.2 l'utilizzo della posta elettronica e di Internet nel rapporto di lavoro

Le linee guida per il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet[6], emanate dal Garante, richiamano il datore di lavoro ai principi di necessità, correttezza e pertinenza nel trattamento dei dati relativi alle navigazioni Internet e alle comunicazioni e-mail effettuate dai lavoratori, e forniscono concrete indicazioni in ordine all'uso del computer sul luogo di lavoro.

Il Garante prescrive ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Grava quindi sul datore di lavoro l'onere di:

- indicare chiaramente ed in modo particolareggiato le corrette modalità di utilizzo da parte dei lavoratori degli strumenti messi a disposizione;
- indicare le modalità e le finalità di eventuali controlli. Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive (ad esempio per rilevare anomalie o per manutenzioni) e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (articolo 4, secondo comma, statuto dei lavoratori legge n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Per uniformarsi a tale prescrizione il datore di lavoro sceglie la modalità informativa più consona a seconda del genere e della complessità delle attività svolte e della dimensione della struttura, e tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

Per le realtà aziendali complesse, il Garante raccomanda l'adozione di un disciplinare interno[7], definito coinvolgendo anche le rappresentanze sindacali, nel quale ad esempio siano indicati:

---

[6] Provvedimento n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007 - doc. web n. 1387522

[7] Vedi il modello di disciplinare nel capitolo "i modelli" al punto 4.9.

- i comportamenti eventualmente non tollerati (ad esempio il download di software o di file musicali, o la tenuta di file privati nella rete interna);
- le modalità ed i tempi in cui sia eventualmente consentito l'utilizzo personale dei servizi di posta elettronica o di rete;
- le informazioni memorizzate temporaneamente (ad esempio le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- le informazioni eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
- le modalità e le finalità di eventuali controlli (precisando ad esempio se, in caso di abusi singoli o reiterati, vengano inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- le conseguenze, anche di tipo disciplinare, che il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet siano utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di sua assenza programmata (ad esempio sistemi di risposta automatica dei messaggi ricevuti, contenente le "coordinate" di altri soggetti cui rivolgersi);
- l'eventuale possibilità di utilizzare i servizi per uso privato con pagamento a carico del lavoratore;
- le misure speciali per particolari realtà lavorative in cui i lavoratori siano tenuti al segreto professionale;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi, adottate ai sensi del Regolamento europeo.

Oltre al disciplinare interno, alle realtà aziendali complesse è raccomandata l'adozione di misure organizzative e tecnologiche, consigliate nel provvedimento, volte a prevenire il rischio di utilizzi impropri.

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 alle condizioni previste dallo Statuto dei lavoratori.

A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili. È quindi vietato:

- effettuare la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riprodurre ed eventualmente memorizzare in modo sistematico le pagine web visualizzate dal lavoratore;
- leggere e registrare i caratteri inseriti tramite la tastiera o analogo dispositivo;
- effettuare l'analisi occulta di computer portatili affidati in uso.

2.3 l'attività promozionale e il contrasto allo spam

Le "Linee guida in materia di attività promozionale e contrasto allo spam"[8] sono finalizzate a combattere il marketing selvaggio e favorire pratiche commerciali "amiche" di utenti e consumatori.

Il provvedimento pone una particolare attenzione alle nuove frontiere dello spamming, quale quello diffuso sui social network (il cosiddetto social spam) o tramite alcune pratiche di "marketing virale" o "marketing mirato", che possono comportare modalità sempre più insidiose e invasive della sfera personale degli interessati.

Di seguito, i principi contenuti nelle Linee guida in materia di offerte commerciali e spam.

Per poter inviare comunicazioni promozionali e materiale pubblicitario tramite sistemi automatizzati (telefonate preregistrate, e-mail, fax, sms, mms) è necessario aver prima acquisito il consenso dei destinatari (cosiddetto opt-in). Tale consenso deve essere specifico, libero, informato e documentato per iscritto.

Il consenso del destinatario è necessario per inviare messaggi promozionali agli utenti di Facebook, Twitter e altri social network (ad esempio pubblicandoli sulla loro bacheca virtuale) o di altri servizi di messaggistica e Voip sempre più diffusi come Skype, WhatsApp, Viber, Messenger, etc. Il fatto che i dati siano accessibili in rete non significa che possano essere liberamente usati per inviare comunicazioni promozionali automatizzate o per altre attività di marketing "virale" o "mirato".

Non è necessario il consenso per inviare e-mail o sms con offerte promozionali ad amici a titolo personale (il cosiddetto "passaparola").

Il Garante consente il **"soft spam"** anche senza consenso, e cioè l'invio di messaggi promozionali, tramite e-mail, ai propri clienti su beni o servizi analoghi a quelli già acquistati. In tal caso si applica la deroga prevista dall'art. 130 comma 4 del Codice della privacy, in base alla quale, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato. Ciò, però, sempre che si tratti di prodotti o servizi analoghi a quelli oggetto della vendita e che l'interessato, adeguatamente informato, non rifiuti tale uso.

Una impresa può inviare offerte commerciali ai propri "follower" sui social network quando dalla loro iscrizione alla pagina aziendale si evinca chiaramente l'interesse o il consenso a ricevere messaggi pubblicitari concernenti il marchio, il prodotto o il servizio offerto.

Il consenso prestato per l'invio di comunicazioni commerciali tramite modalità automatizzate (come e-mail o sms) copre anche quelle effettuate tramite posta cartacea o con telefonate tramite operatore.

2.4 la fidelizzazione dei clienti

Con uno specifico provvedimento[9] del 2005, il Garante ha stabilito le regole per i programmi di fidelizzazione, stabilendo alcuni principi necessari al fine di rendere i

[8] Provvedimento del 4 luglio 2013, pubblicato nella GU n. 174 del 26 luglio 2013 - doc. web n. 2542348

[9] Provvedimento del 24 febbraio 2005 - doc. web n. 1103045

trattamenti di dati personali, raccolti attraverso tessere o carte di fidelizzazione, conformi alla normativa sulla protezione dei dati.

I sistemi e programmi informatici utilizzati per effettuare tali trattamenti devono essere configurati in modo da minimizzare l'utilizzo di informazioni relative a clienti identificabili. In applicazione del principio di necessità, viene considerato illecito il trattamento di dati della clientela se la profilazione può essere perseguita con dati anonimi.

Nel rispetto del principio di proporzionalità, tutti i dati personali devono essere pertinenti e non eccedenti rispetto alle finalità perseguite.

Possono essere trattati solo i dati necessari per attribuire i vantaggi connessi all'utilizzo della carta, e cioè:

- dati anagrafici dell'intestatario della carta;
- dati relativi al volume di spesa globale progressivamente realizzato, se necessari per l'attribuzione dei vantaggi medesimi e per il solo tempo a ciò strettamente necessario. L'eventuale conservazione di dati di dettaglio relativi alle particolari tipologie di beni o servizi acquistati, o di vantaggi conseguiti (punti, premi, bonus, ecc,) non è di regola considerata necessaria per la sola finalità di fidelizzazione; nei casi particolari in cui la conservazione è lecita, deve essere rispettato il principio di proporzionalità.

L'attività di profilazione della clientela può essere svolta solo con dati anonimi e non identificativi, senza una relazione tra i dati che permetta di individuare il cliente e la sua sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo).

Se la finalità può essere perseguita con tali modalità, non è lecito utilizzare e conservare dati personali o identificativi. Negli altri casi, le informazioni acquisite e le modalità del trattamento devono essere pertinenti e non eccedenti rispetto alla tipologia dei beni commercializzati o dei servizi resi.

Non è lecito utilizzare a fini di profilazione dati particolari (ex dati sensibili).

È consentito utilizzare i dati, pertinenti e non eccedenti, dei titolari della carta o dei suoi familiari, o di persone da essi indicate, per comunicazioni commerciali o per la vendita diretta, previo consenso differenziato dei diretti interessati.

Prima del conferimento dei dati e del rilascio della carta deve essere fornita al cliente un'informativa chiara e completa, con modalità non suscettibili di incidere sulla libera scelta del cliente. Deve contenere tutti gli elementi richiesti dalla normativa vigente, senza rimandare a "regolamenti di servizio", e deve essere agevolmente individuabile.

L'eventuale attività di profilazione e/o marketing deve essere posta in specifica evidenza, come pure l'intenzione di cedere a terzi specificamente individuati i dati per finalità da indicare puntualmente.

Deve risultare chiara la circostanza che, per gli scopi ulteriori, il conferimento dei dati ed il consenso sono liberi e facoltativi rispetto alla fidelizzazione in senso stretto.

Per ottenere la carta di fidelizzazione e fruire dei relativi vantaggi il cliente accetta condizioni contrattuali predisposte dall'emittente-titolare del trattamento. **Il consenso del cliente al trattamento dei dati conferiti per la fidelizzazione non è quindi necessario**, e pertanto non è corretto da parte dell'emittente sollecitare un inutile consenso.

È invece necessario il consenso specifico, informato e differenziato, per ogni altra finalità del trattamento che comporti l'identificabilità degli interessati

(profilazione e ricerche di mercato, marketing). L'adesione all'iniziativa di fidelizzazione non può essere condizionata alla manifestazione di tale consenso.

Non è lecito raccogliere un consenso generale, comprendendo anche i casi in cui il consenso non è necessario, o a prescindere dalle finalità perseguite.

Per le comunicazioni in forma elettronica o sistemi automatizzati occorre uno specifico consenso.

I titolari del trattamento devono individuare termini massimi di conservazione dei dati, tenendo conto del fatto che i dati non necessari agli scopi per i quali sono trattati vanno cancellati o trasformati in forma anonima.

In ogni caso **i dati relativi al dettaglio degli acquisti relativi a clienti individuabili possono essere conservati per finalità di profilazione o marketing per un periodo non superiore rispettivamente a 12 o 24 mesi**.

In caso di ritiro, disabilitazione per mancato utilizzo, scadenza o restituzione della carta, deve essere individuato un termine di conservazione dei dati personali a soli fini amministrativi non superiore a 3 mesi

Restano ovviamente fermi gli altri obblighi imposti dal Regolamento e dal Codice della privacy, tra cui, ricordiamo, l'adozione di misure di sicurezza.

2.5 la profilazione dei clienti da parte delle strutture ricettive

Il Garante della privacy, nel corso di accertamenti effettuati in ambiti alberghieri[10], ha ritenuto non conformi alla normativa di protezione dei dati alcuni specifici trattamenti.

Le ispezioni hanno riguardato i seguenti trattamenti (diversi rispetto a quelli obbligatori per legge ed a quelli indispensabili per dar corso al contratto d'albergo) da parte di aziende alberghiere:

- definizione dei profili dei clienti;
- attuazione di operazioni a premio, attraverso apposito programma;
- svolgimento di attività di marketing, limitata ai clienti aderenti al programma di operazione a premio;
- trattamento di dati personali riferiti a soggetti iscritti on-line alla newsletter della società.

Nelle considerazioni pubblicate a seguito delle ispezioni, il Garante ha rinviato ai principi contenuti nel provvedimento generale sulle "Fidelity card"[11] (vedi punto 2.4), nel quale si evidenzia la necessità che il cliente sia preventivamente informato sull'uso dei suoi dati, ed esprima uno specifico consenso. Anche nel settore ricettivo, nell'ambito dei programmi di fidelizzazione, i dati relativi ai gusti, abitudini, durata dei pernottamenti, ed ogni altra informazione utile per conoscere meglio il cliente e anticiparne le richieste, possono essere raccolti e rielaborati solo rispettando le prescrizioni della normativa vigente.

I sistemi e i programmi informatici utilizzati per effettuare tali trattamenti devono essere configurati in modo da minimizzare l'utilizzo di informazioni relative a clienti

[10] Provvedimento 9 marzo 2006, doc. web n. 1252220 e provvedimento 31 gennaio 2008, doc web n. 1490553

[11] Provvedimento del 24 febbraio 2005 - doc. web n. 1103045

identificabili. In applicazione del principio di necessità, viene considerato illecito il trattamento di dati della clientela se la profilazione può essere perseguita con dati anonimi.

Nel rispetto del principio di pertinenza e proporzionalità, il Garante ha segnalato la necessità che siano identificati tempi massimi di conservazione dei dati alla luce delle finalità in concreto perseguite. In particolare, per le seguenti operazioni il Garante ha indicato i tempi congrui:

- realizzazione delle operazioni a premio - possono essere conservati i dati relativi al solo ammontare degli esborsi effettuati sino al conseguimento da parte del cliente del vantaggio previsto, e comunque non oltre la scadenza del termine dell'operazione a premio indicata nel relativo regolamento;
- **creazione dei profili dei clienti - risulta congrua la conservazione dei dati per 12 mesi decorrenti dalla registrazione delle informazioni.**

Nel caso in cui vi siano diverse modalità di raccolta delle informazioni della clientela – in occasione del soggiorno in albergo, con l'adesione all'operazione a premio, mediante la compilazione di modelli resi disponibili on-line – in ciascuna circostanza, e indipendentemente dal mezzo di volta in volta utilizzato, debbono essere rese le informazioni sul trattamento previste dal Regolamento europeo.

Il Garante ha ricordato **la necessità di acquisire uno specifico ed informato consenso dell'interessato nel caso di trattamento per ulteriori finalità di marketing o di definizione dei profili dei clienti**. **Il consenso non è invece necessario con riguardo ai dati trattati in base ad obblighi di legge** (ad esempio per assolvere ad obblighi contabili e tributari o all'obbligo previsto dall'art. 109 TULPS). **Non occorre inoltre il consenso per le operazioni di trattamento finalizzate all'esecuzione del contratto** – ivi comprese quelle derivanti dall'operazione a premio - **o per adempiere, anche in fase precontrattuale, a specifiche richieste del cliente.**

Devono invece essere individuate specifiche modalità che consentano ai clienti di esprimere liberamente e specificamente, anche nei modelli on−line, le proprie scelte in ordine allo svolgimento da parte dell'albergo di attività di marketing, trattandosi di una finalità differente da quella concernente la prestazione alberghiera.

Gli interessati devono essere messi in grado di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei loro dati, manifestando il proprio consenso per ciascuna diversa finalità perseguita dal titolare del trattamento.

Nel caso di prenotazione on line, i moduli di acquisizione dei dati presenti nel sito web dell'albergo devono infatti consentire al cliente di esprimere un consenso libero e specifico al trattamento dei dati a scopo commerciale, rendendo possibile l'acquisizione di un consenso specifico per il suo perseguimento (ad esempio, predisponendo un distinto check box per chi, oltre a richiedere il servizio, intenda autorizzare il titolare del trattamento allo svolgimento di tale attività).

Ai sensi del testo previgente del Codice sulla privacy, nel caso di operazioni di trattamento, effettuate con l'ausilio di strumenti elettronici, finalizzate ad analizzare preferenze e scelte di consumo degli interessati, occorreva effettuare la notificazione al Garante, in quanto considerate tra i trattamenti che mettono a rischio diritti e libertà dell'interessato. La notificazione al Garante è stata abrogata a seguito dell'entrata in vigore del Regolamento europeo. La profilazione anonima non era invece considerata come trattamento che mette a rischio diritti e libertà dell'interessato, e quindi non era soggetta alla notificazione al Garante.

Ricordiamo che il Regolamento europeo, per i trattamenti che mettono a rischio diritti e libertà dell'interessato, qual è considerata **la profilazione non anonima,** prevede ora **l'obbligo di tenere il registro dei trattamenti** anche se si hanno meno di 250 dipendenti (vedi punto 1.13). Facciamo inoltre presente che se per i trattamenti di profilazione non anonima **potrebbe rendersi necessaria l'effettuazione della valutazione di impatto preventiva** (DPIA) di cui al punto 1.10.

2.6 la videosorveglianza

Con un provvedimento dell'8 aprile 2010[12], che sostituisce un precedente provvedimento del 2004[13], il Garante per la protezione dei dati personali ha emanato alcune disposizioni in materia di videosorveglianza.

La prima parte del provvedimento richiama alcuni principi generali ed illustra le prescrizioni applicabili a tutti i sistemi di videosorveglianza. La seconda parte illustra invece le prescrizioni riguardanti specifici trattamenti di dati. Per casi particolari, l'Autorità si riserva di intervenire di volta in volta con atti ad hoc.

Nell'ambito del principio del "bilanciamento degli interessi", il provvedimento stabilisce che **la rilevazione delle immagini può avvenire senza consenso degli interessati quando sia effettuata per perseguire un legittimo interesse del titolare o per fini di tutela delle persone e dei beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo o per finalità di prevenzione incendi o di sicurezza del lavoro.**

La videosorveglianza è quindi ammessa in presenza di concrete situazioni che la giustifichino, a protezione delle persone, della proprietà o del patrimonio aziendale.

Nell'uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, **aree esterne ad edifici e immobili** (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza) il trattamento deve essere effettuato con modalità tali da **limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari non rilevanti** (per esempio, vie, esercizi commerciali, edifici, etc.).

Gli interessati devono essere sempre informati che stanno per accedere ad una zona videosorvegliata. A tal fine, può essere utilizzato un cartello con informazioni minime, riportante il nome del titolare del trattamento e la finalità perseguita. Tale cartello:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

[12] Provvedimento dell'8 aprile 2010, GU n. 99 del 29 aprile 2010 - doc. web n. 1712680

[13] Provvedimento del 29 aprile 2004 – doc. web n.1003482

Il Garante ritiene auspicabile che l'informativa, se resa in forma semplificata (anche avvalendosi del modello allegato al provvedimento), sia disponibile in un testo completo con modalità facilmente accessibili e anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).

In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dal Regolamento europeo.

Deve inoltre essere resa nota agli interessati la circostanza che il sistema di videosorveglianza sia collegato direttamente con le forze di polizia (utilizzando eventualmente lo specifico modello semplificato allegato al provvedimento).

Tale trattamento, nella generalità dei casi, non richiede una valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment), all'esito della quale potrebbe essere necessario consultare l'Autorità Garante per ottenere indicazioni su come gestire il rischio residuale. La DPIA potrebbe invece essere necessaria quando vi è l'associazione delle immagini a dati biometrici o l'uso di sistemi "intelligenti" in grado di rilevare automaticamente comportamenti o eventi anomali (vedi elenco al punto 1.10).

Come regola generale, i dati raccolti mediante la videosorveglianza devono essere protetti per ridurre al minimo i rischi di distruzione, perdita accidentale, accessi non autorizzati o trattamenti non consentiti. Il Garante consiglia fortemente, specie nelle aziende di minori dimensioni, che alle immagini acceda unicamente il titolare al fine di evitare l'individuazione di specifiche figure autorizzate e l'adozione di misure organizzative per verificarne l'attività. All'aumentare della dimensione aziendale, viceversa, dovranno essere adottati:

- diversi livelli di visibilità e trattamento delle immagini (designazione per iscritto di un numero delimitato di incaricati ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui ciò sia indispensabile, a visionare le immagini; individuazione dei diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore distinguendo tra chi è unicamente abilitato a visionare le immagini da chi può effettuare ulteriori operazioni) anche attraverso l'attribuzione di credenziali di autenticazione che abilitino ad effettuare unicamente le operazioni di propria competenza;
- accorgimenti per limitare la possibilità, per i soggetti abilitati, di visionare le immagini registrate e di effettuare sulle stesse operazioni di cancellazione e duplicazione;
- accorgimenti per garantire la cancellazione anche automatica delle registrazioni dopo 24 ore dalla rilevazione. Solo in alcuni casi (come i mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (il provvedimento cita come esempio le banche ma si ritiene che possano essere ricomprese anche altre attività come le gioiellerie) può ritenersi ammesso un periodo più lungo comunque non eccedente la settimana;
- accorgimenti per garantire, nel caso di interventi di manutenzione, che i soggetti a ciò preposti possano accedere alle immagini soltanto se questo si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti abilitati alla visione delle immagini;
- accorgimenti contro il rischio di accesso abusivo alle reti informatiche nel caso di apparati digitali connessi a reti informatiche;

- accorgimenti per l'applicazione di tecniche crittografiche nel caso di trasmissione tramite una rete pubblica di comunicazioni.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura dell'esercizio, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, il Garante ritiene non debba comunque superare la settimana.

Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e deve comunque essere preventivamente sottoposto alla verifica del Garante.

Nel caso di sistemi integrati di videosorveglianza, in cui si effettua la videosorveglianza remota da parte di vari soggetti (società di vigilanza, Internet e service providers, fornitori di video specialistici, ecc.) oltre alle forze di polizia:

- devono essere adottati sistemi per la registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate con conservazione non inferiore a sei mesi;
- deve essere predisposta una separazione logica delle immagini registrate dai diversi titolari.

Nel caso in cui le misure sopra riportate non siano integralmente applicabili per la natura e le caratteristiche dei sistemi di videosorveglianza utilizzati, il titolare dovrebbe effettuare la DPIA, consultando poi eventualmente il Garante.

Nel caso in cui con gli impianti di videosorveglianza sia possibile il controllo a distanza dell'attività dei lavoratori, occorre osservare le garanzie previste dallo Statuto dei lavoratori. Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro.

Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice della privacy, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione.

Le attività di **rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso webcam, devono avvenire con modalità che rendano non identificabili i soggetti ripresi.** Ciò in considerazione del concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi

dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

2.7 l'uso dei cookie

Il Garante, con un provvedimento[14] adottato al termine di una consultazione pubblica, ha regolamentato gli aspetti di protezione dei dati personali connessi con l'installazione dei cookie per finalità di profilazione e marketing da parte dei gestori dei siti web.

I cookie sono piccoli file di testo che i siti visitati inviano al terminale (computer, tablet, smartphone, notebook) dell'utente, dove vengono memorizzati, per poi essere ritrasmessi agli stessi siti alla visita successiva. Sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni sui siti (senza l'uso dei cookie "tecnici" alcune operazioni risulterebbero molto complesse o impossibili da eseguire). Ma attraverso i cookie si può anche monitorare la navigazione, raccogliere dati su gusti, abitudini, scelte personali che consentono la ricostruzione di dettagliati profili dei consumatori.

Il provvedimento stabilisce prescrizioni che variano sulla base delle finalità perseguite da chi li utilizza. L'obbligo di acquisire il consenso preventivo e informato degli utenti è previsto solo in caso di installazione di cookie utilizzati per finalità diverse da quelle meramente tecniche.

Si individuano pertanto due macro-categorie: cookie "tecnici" e cookie "di profilazione".

cookie tecnici - I cookie tecnici sono quelli utilizzati al solo fine di "effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio". Essi non vengono utilizzati per scopi ulteriori e sono normalmente installati direttamente dal titolare o gestore del sito web. Possono essere suddivisi in:

- cookie di navigazione o di sessione, che garantiscono la normale navigazione e fruizione del sito web (permettendo, ad esempio, di realizzare un acquisto o autenticarsi per accedere ad aree riservate);
- cookie analytics, assimilati ai cookie tecnici laddove utilizzati direttamente dal gestore del sito per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come questi visitano il sito stesso;
- cookie di funzionalità, che permettono all'utente la navigazione in funzione di una serie di criteri selezionati (ad esempio, la lingua, i prodotti selezionati per l'acquisto) al fine di migliorare il servizio reso allo stesso.

Per l'uso di tali cookie non è richiesto il preventivo consenso degli utenti, mentre resta fermo l'obbligo di dare l'informativa[15] ai sensi della normativa vigente, che il gestore del sito potrà fornire con le modalità che ritiene più idonee.

cookie di profilazione - I cookie di profilazione sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze

[14] Provvedimento del 8 maggio 2014, GU n. 126 del 3 giugno 2014 - doc. web n. 3118884

[15] Vedi il modello di informativa per il sito web nel capitolo "i modelli", al punto 4.4.

manifestate dallo stesso nell'ambito della navigazione in rete. In ragione della particolare invasività che tali dispositivi possono avere nell'ambito della sfera privata degli utenti, la normativa europea e italiana prevede che **l'utente debba essere adeguatamente informato sull'uso degli stessi ed esprimere il proprio valido consenso**.

Nel caso di uso di cookie di profilazione, per proteggere la privacy degli utenti che navigano sui siti e consentire loro scelte più consapevoli, il Garante ha dunque stabilito che, quando si accede alla home page o ad un'altra pagina di un sito web deve immediatamente comparire un **banner ben visibile**, in cui sia indicato chiaramente:

- che il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati;
- che il sito consente anche l'invio di cookie di "terze parti", ossia di cookie installati da un sito diverso tramite il sito che si sta visitando;
- un link a una informativa più ampia, con le indicazioni sull'uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei cookie di "terze parti";
- l'indicazione che proseguendo nella navigazione (ad esempio, accedendo ad un'altra area del sito o selezionando un'immagine o un link) si presta il consenso all'uso dei cookie.

Per quanto riguarda l'obbligo di tener traccia del consenso dell'utente, al gestore del sito è consentito utilizzare un cookie tecnico, in modo tale da non riproporre l'informativa breve alla seconda visita dell'utente.

L'utente mantiene, comunque, la possibilità di modificare le proprie scelte sui cookie attraverso l'informativa estesa, che deve essere linkabile da ogni pagina del sito.

3. ANALISI DEI TRATTAMENTI TIPICI DELLE AZIENDE RICETTIVE

3.1 prenotazione e fornitura di servizi di alloggio e accessori

Per la definizione dell'accordo contrattuale e per la sua successiva attuazione, la struttura ricettiva acquisisce alcuni dati personali dei **clienti** e degli **ospiti**.

categorie di dati - generalità e recapiti, codice fiscale e/o partita Iva, dati bancari, estremi carte di credito e debito forniti a garanzia e/o a saldo, elenco servizi e prodotti richiesti e acquistati, data di arrivo e partenza, eccetera.

base giuridica – tali trattamenti sono necessari per la definizione dell'accordo contrattuale e per la sua successiva attuazione. Non è necessario acquisire il consenso dell'interessato, trattandosi di trattamenti effettuati nell'ambito dei normali adempimenti precontrattuali e contrattuali. Nel caso in cui oltre ai normali dati personali vengano conferiti anche dati particolari (ad esempio, nel caso di richieste particolari che possano far desumere una malattia o un handicap, la religione professata, l'appartenenza ad un gruppo politico o ad un sindacato, eccetera), riteniamo che non occorra acquisire il consenso per il trattamento da effettuare per fornire il servizio richiesto, mentre invece riteniamo necessario il consenso se il dato particolare viene conservato negli archivi anche dopo la partenza del cliente (o viene comunicato a soggetti esterni all'azienda).**informativa** - all'atto dell'acquisizione dei dati personali del cliente, occorre fornire una corretta informativa sul trattamento, concisa, trasparente, intelligibile. Occorre informare il cliente che non è richiesto il suo consenso (tranne nel caso in cui siano conferiti dati particolari, ex "sensibili"). In caso di rifiuto a conferire i dati personali, tutti o alcuni servizi non potranno essere forniti.

conservazione dei dati - occorre informare il cliente che il trattamento cesserà alla sua partenza, ma alcuni suoi dati personali potranno o dovranno continuare ad essere trattati per obblighi di legge (per 10 anni ai sensi dell'articolo 2220 del codice civile, e anche oltre in caso di contenzioso).

principi di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer). Inoltre, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti, o nel caso di trattamenti che mettano a rischio diritti e libertà dell'interessato).

3.2 registrazione a fini di polizia

L'articolo 109 del Testo Unico delle leggi di pubblica sicurezza[16] stabilisce che i gestori di strutture ricettive non possono dare alloggio a persone sfornite di documento di riconoscimento. Inoltre, i gestori sono obbligati a comunicare alle questure, avvalendosi di mezzi informatici o telematici o mediante fax, le generalità delle **persone alloggiate**, secondo modalità stabilite con uno specifico decreto ministeriale[17].

categorie di dati - generalità ed estremi dei documenti di riconoscimento, data di arrivo e notti di pernottamento, relazioni di parentela.

base giuridica – non è richiesto il consenso dell'interessato trattandosi di un trattamento effettuato in esecuzione ad un obbligo di legge.

informativa - all'atto dell'acquisizione delle generalità, va data al cliente una corretta informativa sul trattamento, concisa, trasparente, intelligibile. Occorre informare il cliente che il conferimento dei dati è obbligatorio ed il trattamento non richiede il suo consenso, ed in caso di rifiuto a fornirli non potrà essere ospitato nella struttura ricettiva.

conservazione dei dati - i dati acquisiti per tale finalità non possono essere conservati presso la struttura ricettiva, a meno che il cliente non fornisca specifica autorizzazione.

principio di liceità – i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer). Inoltre, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti).

[16] Approvato con RD 18 giugno 1931, n.773.

[17] Decreto del Ministero dell'Interno 7 gennaio 2013 "Disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive".

3.3 conservazione dei dati registrati a fini di polizia

Il decreto del Ministero dell'Interno 7 gennaio 2013, che disciplina le modalità di invio alle questure dei dati dei clienti alloggiati, prevede che i dati notificati ai sensi dell'articolo 109 del Tulps siano cancellati dalla struttura ricettiva subito dopo l'effettuazione dell'invio alle questure. I **clienti abituali** possono però richiedere alla struttura ricettiva di conservare i dati, al fine di accelerare le procedure di check in in caso di successivi soggiorni.

categorie di dati - generalità ed estremi dei documenti di riconoscimento.

base giuridica – è necessario il consenso dell'interessato.

informativa - all'atto dell'acquisizione delle generalità, va data al cliente l'informativa sul trattamento, concisa, trasparente, intelligibile. Occorre informare il cliente che per tale finalità è necessario il consenso, revocabile in qualsiasi momento.

conservazione dei dati – occorre stabilire un termine massimo per la conservazione di tali dati, da riportare nella informativa.

principio di liceità – i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer). Inoltre, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti).

3.4 il servizio di ricevimento e portineria

La funzione di ricevimento di messaggi e telefonate indirizzati al **cliente** durante il suo soggiorno comporta la comunicazione all'esterno di informazioni relative al soggiorno del cliente stesso.

categorie di dati - generalità, presenza presso la struttura ricettiva, eccetera.

base giuridica – per comunicare all'esterno informazioni sulla presenza del cliente, all'atto del ricevimento di telefonato o messaggi, è necessario acquisire il suo consenso.

informativa - va data una corretta informativa sul trattamento, concisa, trasparente, intelligibile. Il cliente va informato della possibilità di revocare il consenso in qualsiasi momento.

conservazione dei dati - il trattamento cessa alla partenza del cliente (tranne in caso di richieste specifiche del cliente stesso).

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – Il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer). Inoltre, sempre che ci si limiti alla funzione di ricevimento di telefonate e messaggi, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti).

3.5 trattamento di dati per adempiere agli obblighi amministrativi, contabili e fiscali

Molte norme richiedono all'imprenditore di conservare in azienda e/o di inviare a enti pubblici dati personali a fini amministrativi, contabili o fiscali. Tra queste, ricordiamo la norma generale di cui all'articolo 2220 del codice civile, che prevede la conservazione delle scritture contabili per 10 anni. Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti (e quindi tutta la corrispondenza intercorsa con il cliente e la relativa documentazione fiscale).

categorie di dati - generalità e recapiti, codice fiscale e/o partita Iva, estremi carte di credito e debito forniti a saldo, servizi e prodotti acquistati riportati negli estratti conto e nei documenti fiscali, eccetera.

base giuridica – non è richiesto il consenso dell'interessato trattandosi di trattamenti effettuati in esecuzione ad obblighi di legge.

informativa - va data una corretta informativa sul trattamento, concisa, trasparente, intelligibile. L'interessato va informato che per tali finalità il trattamento è effettuato senza necessità di acquisire il suo consenso. Occorre inoltre informarlo che alcuni dati vengono comunicati a terzi in adempimento ad obblighi di legge (ad esempio lo "spesometro", eccetera), e che in caso di rifiuto a conferire i dati necessari per gli adempimenti sopra indicati, non potranno essere forniti i servizi richiesti.

conservazione dei dati - occorre informare l'interessato che per tali finalità i dati vengono conservati presso la struttura ricettiva per il tempo previsto dalle rispettive normative (10 anni, e anche oltre in caso di accertamenti fiscali o contenziosi).

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – Il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer). Inoltre, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti, o nel caso di trattamenti che mettano a rischio diritti e libertà dell'interessato).

3.6 le iniziative promozionali e pubblicitarie

Molto spesso le aziende ricettive conservano i dati e recapiti dei clienti, acquisiti nel momento della prenotazione o al momento dell'arrivo, e li utilizzano per inviare periodicamente gli aggiornamenti delle proprie tariffe, pubblicizzare offerte speciali, o semplicemente inviare gli auguri per il compleanno o per le festività, sempre comunque con fine promozionale.

categorie di dati - generalità, indirizzi postali e/o elettronici , eccetera.

base giuridica – per tale finalità il cliente deve esprimere il consenso, revocabile in qualsiasi momento.

informativa - va data una corretta informativa sul trattamento, concisa, trasparente, intelligibile. Il cliente va informato della possibilità di revocare il consenso in qualsiasi momento.

conservazione dei dati – occorre stabilire un termine massimo per la conservazione dei dati.

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer), a meno che non sia effettuato il monitoraggio regolare e sistematico degli interessati su larga scala. Inoltre, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti, o nel caso di trattamenti che mettano a rischio diritti e libertà dell'interessato).

3.7 i programmi di fidelizzazione dei clienti

Alcune aziende trattano dati dei clienti nell'ambito dei programmi di fidelizzazione, attraverso il rilascio di tessere o carte, finalizzati ad attribuire vantaggi ai possessori delle stesse.

categorie di dati - generalità, recapiti, preferenze, eccetera.

base giuridica – per tale finalità il cliente non deve esprimere il consenso, in quanto per ottenere la carta di fidelizzazione e fruire dei relativi vantaggi il cliente accetta le condizioni contrattuali predisposte dall'emittente-titolare del trattamento. L'attività di profilazione della clientela può essere svolta solo con dati anonimi e non identificativi, senza una relazione tra i dati che permetta di individuare il cliente e la sua sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo). È invece necessario il consenso specifico, informato e differenziato, per ogni altra finalità del trattamento che comporti l'identificabilità degli interessati (profilazione e ricerche di mercato, marketing). L'adesione all'iniziativa di fidelizzazione non può essere condizionata alla manifestazione di tale consenso.

informativa - va data una corretta informativa sul trattamento, concisa, trasparente, intelligibile. Il cliente va informato della possibilità di revocare il consenso in qualsiasi momento.

conservazione dei dati – occorre stabilire un termine massimo per la conservazione dei dati.

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer), a meno che non sia effettuato il monitoraggio regolare e sistematico degli interessati su larga scala. Se viene effettuata la profilazione con dati non anonimi potrebbe rendersi necessaria l'effettuazione della valutazione di impatto preventiva (DPIA) di cui al punto 1.10.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti, o nel caso di profilazione con dati non anonimi, in quanto tale trattamento è considerato tra quelli che mettono a rischio diritti e libertà dell'interessato).

3.8 la videosorveglianza

Alcune aziende installano sistemi di videosorveglianza, con o senza registrazione delle immagini, per motivi di sicurezza. Poiché le aziende sono anche luoghi di lavoro, oltre alla normativa sulla privacy occorre rispettare anche le prescrizioni dello Statuto dei lavoratori.

categorie di dati - immagini

base giuridica – per tale trattamento non è richiesto il consenso dei soggetti interessati, in quanto si persegue il legittimo interesse dell'azienda a tutelare le persone ed i beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e per finalità di prevenzione incendi e di sicurezza del lavoro.

informativa - occorre informare clienti, ospiti e lavoratori nel caso in cui sia installato un sistema di videosorveglianza in alcune aree della struttura ricettiva, individuabili per la presenza di appositi cartelli, e se le immagini siano o meno registrate. Occorre inoltre informare che per tale trattamento non è richiesto il consenso. Nel caso in cui le immagini siano registrate, occorre informare che si provvede alla loro cancellazione nei termini previsti dal Garante (dopo 24 ore, salvo festivi o altri casi di chiusura dell'esercizio, e comunque non oltre una settimana) e che non sono oggetto di comunicazione a terzi, tranne nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

conservazione dei dati – cancellazione nei termini previsti dal Garante (dopo 24 ore, salvo festivi o altri casi di chiusura dell'esercizio, e comunque non oltre una settimana) tranne nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Non riteniamo generalmente necessaria la designazione del responsabile della protezione dei dati (DPO - Data Protection Officer), a meno che non sia effettuato il monitoraggio regolare e sistematico degli interessati su larga scala. Inoltre, nella generalità dei casi non è richiesta una valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) di cui al punto 1.10. La DPIA potrebbe invece essere necessaria quando vi è l'associazione delle immagini a dati biometrici o l'uso di sistemi "intelligenti" in grado di rilevare automaticamente comportamenti o eventi anomali.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti, o nel caso di trattamenti che mettono a rischio diritti e libertà dell'interessato).

3.9 trattamento dei dati relativi ai lavoratori

I dati personali del lavoratore possono essere trattati dal datore di lavoro nella misura in cui ciò sia necessario per dare corretta esecuzione al rapporto di lavoro. Le informazioni trattate devono essere pertinenti e non eccedenti le finalità perseguite, e devono essere osservate tutte le disposizioni della normativa italiana ed europea.

categorie di dati - dati anagrafici dei lavoratori, nonché altre informazioni connesse allo svolgimento dell'attività lavorativa (la tipologia del contratto, la qualifica, la retribuzione, il tempo di lavoro anche straordinario, ferie e permessi, assenza dal servizio, procedimenti disciplinari, eccetera). È possibile che vengano trattatati dati biometrici e dati particolari (ex "sensibili"), riferiti anche a terzi (credo religioso, adesione a sindacati, dati che rivelano lo stato di salute contenuti in certificati medici o in altra documentazione).

base giuridica – il Regolamento europeo non prevede la necessità di acquisire il consenso del lavoratore, se i trattamenti effettuati sono quelli strettamente necessari 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, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi del lavoratore. Le linee guida del Garante (vedi il punto 2.1), antecedenti l'emanazione del Regolamento europeo, prevedono in alcuni casi la necessità del consenso del lavoratore.

informativa - all'atto dell'acquisizione dei dati del lavoratore, va data una corretta informativa sul trattamento, in forma concisa, trasparente, intelligibile.

conservazione dei dati - occorre informare l'interessato che per tali finalità i dati vengono conservati presso la struttura ricettiva per tutta la durata del rapporto di lavoro e per un periodo successivo secondo le norme vigenti.

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Il Garante ritiene che le piccole e medie imprese non siano obbligate a designare il responsabile della protezione dei dati (DPO - Data Protection Officer) per i trattamenti dei dati personali connessi alla gestione corrente dei rapporti con i dipendenti. Inoltre, nella generalità dei casi non è richiesta una valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment). La DPIA potrebbe invece essere necessaria quando sono trattati dati biometrici.

registro delle attività di trattamento – in alcuni casi il trattamento deve essere inserito in un registro delle attività di trattamento (per le imprese con almeno 250 dipendenti, o nel caso di trattamenti che mettono a rischio diritti e libertà dell'interessato).

3.10 trattamento dei dati relativi ai fornitori

Se i fornitori sono persone giuridiche (ad esempio società di capitali) il trattamento dei relativi dati non ricade nell'ambito di applicazione della normativa sulla protezione dei dati. La tutela prevista dal Regolamento europeo e dal Codice della privacy è infatti assicurata solo nel caso si tratti di dati di persone fisiche. Rientrano però nel campo di applicazione della normativa i dati personali di imprenditori individuali, società di persone e liberi professionisti, anche se si tratta comunque di soggetti che, agendo come professionisti, necessitano sicuramente di minore protezione.

categorie di dati – generalità e recapiti, codice fiscale e/o partita IVA, dati bancari, eccetera.

base giuridica – non è necessario acquisire il consenso dei fornitori, trattandosi di trattamenti effettuati nell'ambito dei normali adempimenti precontrattuali o contrattuali, o in esecuzione di obblighi di legge.

informativa - all'atto dell'acquisizione dei dati del fornitore, va data una corretta informativa sul trattamento, in forma concisa, trasparente, intelligibile.

conservazione dei dati - occorre informare l'interessato che per tali finalità i dati vengono conservati presso la struttura ricettiva per il tempo previsto dalle rispettive normative (10 anni, e anche oltre in caso di contenziosi o accertamenti fiscali).

principio di liceità - i dati personali devono essere trattati in modo lecito, corretto e trasparente, rispettando le prescrizioni del Regolamento e riconoscendo i diritti degli interessati.

valutazione dei rischi e misure tecniche e organizzative per garantire la sicurezza – il trattamento deve essere effettuato previa analisi dei rischi e implementazione delle misure ritenute idonee per limitare tali rischi. Il Garante ritiene che le piccole e medie imprese non siano obbligate a designare il responsabile della protezione dei dati (DPO - Data Protection Officer) per i trattamenti dei dati personali connessi alla gestione corrente dei rapporti con i fornitori. Inoltre, non riteniamo necessaria la valutazione di impatto preventiva (DPIA - Data Protection Impact Assessment) in quanto i trattamenti in oggetto non comportano un rischio elevato per i diritti e le libertà delle persone interessate.

registro delle attività di trattamento – In alcuni casi il trattamento deve essere inserito nel registro delle attività di trattamento (per le imprese con almeno 250 dipendenti).

4. I MODELLI

4.1 informativa al cliente

Il modello che segue, da adattare alla specifica realtà aziendale, è finalizzato ad informare il cliente o ospite sui trattamenti ordinari di dati effettuati dalle strutture ricettive.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Il modello di informativa presume che siano effettuati dalla azienda ricettiva i trattamenti di dati di seguito descritti:

- **Trattamento di dati dei clienti o ospiti acquisiti dalla struttura ricettiva per confermare una prenotazione di servizi di alloggio e servizi accessori, e per fornire i servizi richiesti** (generalità e recapiti, codice fiscale e/o partita Iva, estremi carte di credito e debito forniti a garanzia e/o a saldo, elenco servizi e prodotti richiesti e acquistati, data di arrivo e partenza, eccetera). Tali trattamenti sono necessari per la definizione dell'accordo contrattuale e per la sua successiva attuazione, e pertanto occorre informare il cliente che non è richiesto il suo consenso (tranne nel caso in cui siano conferiti e conservati dati particolari, cosiddetti sensibili). In caso di rifiuto a conferire i dati personali, tutti o alcuni servizi non potranno essere forniti. Occorre informare il cliente che il trattamento cesserà alla sua partenza, ma alcuni suoi dati personali potranno o dovranno continuare ad essere trattati per altre finalità, da indicare specificatamente (descritte di seguito).
- **Trattamento di dati dei clienti o ospiti per adempiere all'obbligo previsto dal "Testo unico delle leggi di pubblica sicurezza"** (articolo 109 R.D. 18.6.1931 n. 773) che impone di comunicare alla Questura, per fini di pubblica sicurezza, le generalità dei clienti alloggiati secondo le modalità stabilite dal Ministero dell'Interno (Decreto 7 gennaio 2013) (generalità ed estremi dei documenti di riconoscimento, data di arrivo e notti di pernottamento, relazioni di parentela, eccetera). Occorre informare il cliente che il conferimento dei dati è obbligatorio ed il trattamento non richiede il suo consenso, ed in caso di rifiuto a fornirli non potrà essere ospitato nella struttura ricettiva. I dati acquisiti per tale finalità non saranno conservati presso la struttura ricettiva, a meno che il cliente non fornisca specifica autorizzazione.
- **Trattamento di dati dei clienti o ospiti per adempiere ai vigenti obblighi amministrativi, contabili e fiscali** (generalità e recapiti, codice fiscale e/o partita Iva, estremi carte di credito e debito forniti a saldo, servizi e prodotti acquistati riportati negli estratti conto e nei documenti fiscali, eccetera). Occorre informare il cliente che per tali finalità il trattamento è effettuato senza necessità di acquisire il consenso del cliente. Occorre inoltre informarlo che alcuni dati vengono comunicati a terzi in adempimento ad obblighi di legge (ad esempio spesometro, eccetera), e che in caso di rifiuto a conferire i dati necessari per gli adempimenti sopra indicati, non potranno essere forniti i servizi richiesti. Occorre infine informare che per tali finalità i dati vengono conservati presso la struttura ricettiva per il tempo previsto dalle rispettive normative (articolo 2220 del codice civile: 10 anni, e anche oltre in caso di contenziosi o accertamenti fiscali).
- **Trattamento di dati dei clienti e ospiti effettuato per accelerare le procedure di registrazione in caso di successivi soggiorni** (generalità, estremi dei documenti di riconoscimento, recapiti, eccetera). Per tale finalità il cliente deve esprimere il consenso, revocabile in qualsiasi momento. L'azienda deve stabilire un termine massimo per la conservazione di tali dati, da riportare nella informativa.

- **Trattamento di dati per espletare la funzione di ricevimento di messaggi e telefonate indirizzati al cliente durante il suo soggiorno** (generalità, presenza presso la struttura ricettiva, eccetera). Per tale finalità è necessario il consenso del cliente. Il cliente va informato della possibilità di revocare il consenso in qualsiasi momento e che il trattamento cesserà comunque alla sua partenza.
- **Trattamento di dati dei clienti e ospiti effettuato per inviare messaggi promozionali** (generalità, recapiti, eccetera). Per tale finalità il cliente deve esprimere il consenso, revocabile in qualsiasi momento. L'azienda deve stabilire un termine massimo per la conservazione di tali dati, da riportare nella informativa.
- **Trattamento di dati per fini di protezione delle persone, della proprietà e del patrimonio aziendale attraverso un sistema di videosorveglianza**. Occorre informare clienti e ospiti nel caso in cui sia installato un sistema di videosorveglianza di alcune aree della struttura ricettiva, individuabili per la presenza di appositi cartelli, e se le immagini siano o meno registrate. Occorre inoltre informare che per tale trattamento non è richiesto il consenso, in quanto persegue il legittimo interesse dell'azienda a tutelare le persone ed i beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e per finalità di prevenzione incendi e di sicurezza del lavoro. Nel caso in cui le immagini siano registrate, occorre informare che si provvede alla loro cancellazione nei termini previsti dal Garante (dopo 24 ore, salvo festivi o altri casi di chiusura dell'esercizio, e comunque non oltre una settimana) e che non sono oggetto di comunicazione a terzi, tranne nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

L'informativa deve essere fornita al cliente all'atto della raccolta di dati personali, sia nella fase di prenotazione sia al momento dell'arrivo presso la struttura ricettiva.

Gentile Cliente,

ai sensi della normativa vigente in materia di protezione dei dati personali (Regolamento UE n. 679 del 2016 - D. Legisl. 196/2003), desideriamo informarla che i trattamenti dei suoi dati personali sono effettuati con correttezza e trasparenza, per fini leciti e tutelando la sua riservatezza ed i suoi diritti.

I trattamenti sono effettuati, anche con l'ausilio di mezzi informatici, da noi e da nostri responsabili e incaricati per le seguenti finalità:

1. *per acquisire e confermare la sua prenotazione di servizi di alloggio e servizi accessori, e per fornire i servizi richiesti. Trattandosi di trattamenti necessari per la definizione dell'accordo contrattuale e per la sua successiva attuazione, non è richiesto generalmente il suo consenso. In caso di rifiuto a conferire i dati personali, non potremo confermare la prenotazione o fornirle i servizi richiesti. Il trattamento cesserà alla sua partenza, ma alcuni suoi dati personali potranno o dovranno continuare ad essere trattati per le finalità e con le modalità indicate nei punti successivi;*
2. *per adempiere all'obbligo previsto dal "Testo unico delle leggi di pubblica sicurezza" (articolo 109 R.D. 18.6.1931 n. 773) che ci impone di comunicare alla Questura, per fini di pubblica sicurezza, le generalità dei clienti alloggiati secondo le modalità stabilite dal Ministero dell'Interno (Decreto 7 gennaio 2013). Il conferimento dei dati*

è obbligatorio e non richiede il suo consenso, ed in caso di rifiuto a fornirli non potremo ospitarla nella nostra struttura. I dati acquisiti per tale finalità non vengono da noi conservati, a meno che non ci fornisca il consenso alla conservazione come previsto al punto 4;

3. *per adempiere ai vigenti obblighi amministrativi, contabili e fiscali. Per tali finalità il trattamento è effettuato senza necessità di acquisire il suo consenso. I dati sono trattati da noi e da nostri responsabili e incaricati, e vengono comunicati all'esterno solo in adempimento ad obblighi di legge. In caso di rifiuto a conferire i dati necessari per gli adempimenti sopra indicati, non potremo fornirle i servizi richiesti. I dati acquisiti per tali finalità vengono da noi conservati per il tempo previsto dalle rispettive normative (10 anni, e anche oltre in caso di accertamenti fiscali);*
4. *per accelerare le procedure di registrazione in caso di suoi successivi soggiorni presso la nostra struttura. Per tale finalità, previa acquisizione del suo consenso revocabile in qualsiasi momento, i suoi dati saranno conservati per il periodo massimo di _____ (inserire un termine**),** e saranno utilizzati quando sarà nuovamente nostro ospite per le finalità di cui ai punti precedenti;*
5. *per espletare la funzione di ricevimento di messaggi e telefonate a lei indirizzati durante il suo soggiorno. Per tale finalità è necessario il suo consenso. Potrà revocare il consenso in qualsiasi momento. Il trattamento cesserà comunque alla sua partenza;*
6. *per inviarle nostri messaggi promozionali e aggiornamenti sulle tariffe e sulle offerte praticate. Per tale finalità, previa acquisizione del suo consenso, i suoi dati saranno conservati per il periodo massimo di _____(inserire un termine), e non saranno comunicati a terzi. Potrà revocare il consenso in qualsiasi momento;*
7. *per fini di protezione delle persone, della proprietà e del patrimonio aziendale attraverso un sistema di videosorveglianza di alcune aree della struttura, individuabili per la presenza di appositi cartelli. Per tale trattamento non è richiesto il suo consenso, in quanto persegue il nostro legittimo interesse a tutelare le persone ed i beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e per finalità di prevenzione incendi e di sicurezza del lavoro. Le immagini registrate sono cancellate dopo 24 ore, salvo festivi o altri casi di chiusura dell'esercizio, e comunque non oltre una settimana. Non sono oggetto di comunicazione a terzi, tranne nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.*

Desideriamo inoltre informarla che il Regolamento europeo le riconosce alcuni diritti, (diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione) se ed in quanto applicabili (articoli da 15 a 22 del Regolamento UE n. 679 del 2016). Può inoltre proporre reclamo all'autorità di controllo, secondo le procedure previste dalla normativa vigente.

Per qualsiasi ulteriore informazione, e per far valere i diritti a lei riconosciuti dal Regolamento europeo, potrà rivolgersi a:

Titolare del trattamento *(nome e cognome o denominazione in caso di ente o società): _____ (dati di contatto) _____*

Responsabile della protezione dei dati - DPO *(nel caso sia stato nominato): (nome e cognome) _____ (dati di contatto) _____*

Dear Customer

In accordance with applicable privacy laws (EU Regulations n. 679, 2016 - D. Legisl. 196/2003, we would like to take this opportunity to inform you that your personal information will be processed in an ethical and transparent manner, only for lawful purposes, and in a manner that safeguards your privacy and your rights.

Processing takes place manually and using IT tools, and is done, by us and our persons in charge of data processing, for the following purposes:

1. *To obtain and confirm your booking of accommodations and other services, and to provide such services as requested. Since this processing is required to define our contractual relationship and to perform under our contract with you, your consent is generally not required. Should you refuse to submit your personal information, we will not be able to confirm your booking or provide you with the requested services. Processing shall cease once you check out, although some of your personal information may (or in some instances, has to) continue to be processed for the purposes and in the manner described below;*
2. *To comply with our "Public Safety Law" (Article 109 Royal Decree n. 773, 18/6/1931) which requires that we provide identification data of our guests to the police, for purposes of public safety, in the manner established by the Ministry of the Interior (Decree of 7 January 2013). Data submission is mandatory, and does not require your consent. Should you refuse to provide such information, we will not be able to host you in our hotel. Data acquired for such purposes shall not be retained by us, unless you provide consent to their retention as required under point 4,* infra*;*
3. *To comply with applicable administrative, accounting, and tax regulations. For these purposes, your consent is not required. Personal information is processed by us and our persons in charge of data processing, and is disclosed outside the company only when and if required by law. Should you refuse to submit the required data for the above purposes, we will not be able to provide you with the requested services. Data acquired for such purposes is retained by us for the required statutory period (10 years – or longer, in case of tax audits);*
4. *To speed-up check-in on your next visit to our hotel. For such purposes, upon obtaining your consent (which can be revoked at any moment), your information will be retained for a maximum of _____(inserire un termine), and will be used the next time you are our guest, for the reasons listed* supra*;*
5. *To allow you to receive messages and telephone calls during your stay. Your consent is required for such purposes. You can revoke your consent at any time. Such processing, where consent is granted, shall end when you check out;*
6. *To send you advertising messages and updates on special rates and promotions. For*

this purpose, upon obtaining your consent, your information shall be retained for a maximum of _____ (inserire un termine), and will not be disclosed to third parties. You may revoke your consent at any moment;

7. *For purposes of protecting persons, property, and company assets, using a video-surveillance system for some areas of the hotel, which are duly identified by signage. Your consent is not required for such processing because it is conducted pursuant to our legitimate interest to safeguard persons and property against potential violence, theft, robbery, damage, and vandalism. Surveillance is also conducted for purposes of fire prevention and occupational safety and health. Recorded images are erased after 24 hours, except on holidays or other days the business is closed; images are never retained for more than one week. These images are not subject to third-party disclosure, except as required to comply with a specific investigatory demands from a court or the police.*

We also would like to inform you that the European Regulation grant you certain rights, including rights of access to, adjustment, erasure, limitation of, or objection to the processing of your data, as well as data portability rights, when and insofar as applicable (Articles 15-22 of the EU Regulations n. 679, 2016). You can also file a complaint with the Data Protection Authority, according to the procedures set forth under applicable regulations.

For any other concern, and to assert your rights under the EU Regulation, please contact:

Data Controller (nome e cognome o denominazione in caso di ente o società): _____ (dati di contatto) _____

Data Protection Officer - DPO (nel caso sia stato nominato): (nome e cognome) _____ (dati di contatto) _____

4.2 acquisizione del consenso all'arrivo del cliente

Il modello, integrato e modificato secondo le specifiche esigenze, può essere fatto sottoscrivere al cliente all'arrivo presso la struttura ricettiva, nel caso in cui siano effettuati i trattamenti che richiedono il consenso (punti 4, 5 e 6 dell'informativa).

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Io sottoscritto …….. ai sensi della normativa vigente in materia di protezione dei dati personali (Regolamento UE n. 679 del 2016 - D. Legisl. 196/2003), ricevuta l'informativa sul trattamento dei miei dati personali:

□ *autorizzo*
□ *non autorizzo*
la struttura ricettiva alla comunicazione esterna di dati relativi al mio soggiorno al fine esclusivo di consentire la funzione di ricevimento di messaggi e telefonate a me indirizzati

□ *autorizzo*
□ *non autorizzo*
la struttura ricettiva alla conservazione delle mie generalità al fine di accelerare le procedure di registrazione in caso di miei successivi soggiorni

□ *autorizzo*
□ *non autorizzo*
la struttura ricettiva ad inviare al mio domicilio o al mio indirizzo di posta elettronica periodica documentazione sulle tariffe e sulle offerte praticate.

Data e firma ……..

I, the undersigned …….., according to the provisions of the applicable privacy regulations (EU Regulations n. 679, 2016 - D. Legisl. 196/2003, having received the privacy notice,

□ *authorize*
□ *do not authorize*
the hotel to the outward communication of information about my stay, with the only aim of permitting the receiving of messages and calls addressed to me

□ *authorize*
□ *do not authorize*
the hotel to retain my information in order to streamline check-in procedures for subsequent stays

□ *authorize*
□ *do not authorize*
the hotel to send periodic advertisements on their rates and special offers to my home address or email address

Date and signature ……..

4.3 informativa e acquisizione del consenso online

Il modello che segue, opportunamente verificato ed integrato, può essere inserito nella modulistica online di prenotazione o richiesta di disponibilità (ferma restando la necessità di fornire l'informativa completa sia sul sito che all'arrivo del cliente, e di richiedere l'eventuale consenso di cui al paragrafo che precede).

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Gentile Cliente,

la informiamo che i dati da lei conferiti saranno trattati con mezzi informatici nel rispetto dei principi stabiliti dalla normativa vigente in materia di protezione di dati (Regolamento UE n. 679 del 2016 - D. Legisl. 196/2003) al solo fine di fornirle le informazioni richieste, ed eventualmente per definire/confermare la prenotazione di camere e altri servizi. L'informativa completa sulle modalità e finalità dei trattamenti effettuati è accessibile attraverso il seguente link_____.

Se è interessato a ricevere in futuro, all'indirizzo da lei indicato, la nostra newsletter/periodiche informative sulle nostre tariffe e offerte speciali, dovrà fornirci apposito consenso. Potrà comunque successivamente, in ogni momento, revocare tale consenso, come indicato nella informativa.

□ *prendo atto dell'informativa sul trattamento dei dati personali*

□ *autorizzo l'invio della newsletter e di periodica documentazione sulle tariffe e sulle offerte praticate presso l'indirizzo da me indicato*

Dear Customer,

please note that data submitted by you shall be processed using electronic means in compliance with the principles set forth in applicable data privacy laws and regulations (EU Regulation n. 679, 2016 - D. Legisl. 196/2003), solely for the purpose of providing you with the information requested, and potentially for placing/confirming your booking of room(s) and other services/amenities. The complete privacy policy on processing methods and purposes is available at the following link _____.

If you are interested in receiving our newsletter / periodic updates on special rates and promotions (to be sent to an address supplied by you), you must provide explicit consent to the same. You may at any time thereafter revoke such consent, as noted in the policy.

□ *I acknowledge receipt of the privacy policy*

□ *I authorise the mailing of newsletters and periodic notices on special rates/promotions to the address I have supplied*

4.4 “privacy policy” del sito web

Riportiamo di seguito un modello di “privacy policy” da inserire nel sito web della struttura ricettiva. Il testo va modificato ed integrato in relazione agli ambiti di operatività ed alle funzioni effettivamente svolte.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

La privacy policy di questo sito

In questa pagina si descrivono le modalità di gestione del sito in riferimento al trattamento dei dati personali degli utenti che lo consultano. Si tratta di un'informativa che è resa anche ai sensi della normativa vigente in materia di protezione dei dati personali (Regolamento (UE) 2016/679 - D. Legisl. 196/2003), a coloro che consultano le pagine del sito internet www. …….. (di seguito: “sito”) o che usufruiscono dei servizi sullo stesso messi a disposizione.

L'informativa è resa esclusivamente per il sito di ……..e non anche per gli altri siti web eventualmente consultati dall'utente tramite i link presenti all'interno del sito.

Titolare del trattamento (nome e cognome o denominazione in caso di ente o società): _____ (dati di contatto) _____

Responsabile della protezione dei dati - DPO (nel caso sia stato nominato): (nome e cognome) _____ (dati di contatto) _____

Tipi di dati trattati

Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento

di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, allo stato i dati sui contatti web non persistono per più di sette giorni[18].

Dati forniti volontariamente dall'utente

La registrazione dei dati personali, anche particolari (cosiddetti "sensibili"), sulla apposita pagina del sito, finalizzata a richiedere servizi, l'accesso alle aree riservate del sito, la richiesta di invio della newsletter, nonché l'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo sito, comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti.

Specifiche informative di sintesi verranno progressivamente riportate o visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta.

Cookie[19]

Nessun dato personale degli utenti viene in proposito acquisito dal sito.

Non viene fatto uso di cookie per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookie persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. cookie di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del sito.

I c.d. cookie di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

Facoltatività del conferimento dei dati

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali riportati nei moduli di richiesta di servizi, o comunque indicati in contatti con i nostri uffici per sollecitare l'invio della newsletter, di materiale informativo o di altre comunicazioni.

Il loro mancato conferimento può comportare l'impossibilità di ottenere quanto richiesto.

Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati e manuali per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Diritti degli interessati

I soggetti cui si riferiscono i dati personali hanno alcuni diritti (diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione) se ed in quanto

[18] Indicare gli effettivi giorni di permanenza dei dati.

[19] Se si fa uso di cookie di profilazione, occorre rispettare quanto indicato dal Garante nel Provvedimento del 8 maggio 2014, GU n. 126 del 3 giugno 2014 - doc. web n. 3118884. Vedi punto 2.7.

applicabili (articoli da 15 a 22 del Regolamento UE n. 679 del 2016). Hanno inoltre diritto di proporre reclamo all'autorità di controllo, secondo le procedure previste dalla normativa vigente.

Le richieste vanno rivolte:

- via e-mail, all'indirizzo: ……

- via fax: ……..

- oppure via posta, a ……..., Via ……

4.5 informativa ai lavoratori

Il modello di informativa che segue, da modificare o integrare a seconda delle specifiche esigenze, va consegnato ai lavoratori o reso loro disponibile.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Ai sensi della normativa vigente in materia di protezione dei dati (Regolamento (UE) 2016/679 - D. Legisl. 196/2003), desideriamo informarla che i trattamenti dei suoi dati personali, anche particolari (ex dati sensibili), da noi acquisiti al momento della assunzione e successivamente, sono effettuati con correttezza e trasparenza, per fini leciti e tutelando la sua riservatezza ed i suoi diritti.

I trattamenti sono effettuati, da noi e da nostri responsabili e incaricati, anche con l'ausilio di mezzi informatici per dare esecuzione al contratto di lavoro e per adempiere agli obblighi previsti dalla legge e dalle diposizioni della contrattazione collettiva. Il suo consenso potrà essere necessario solo per alcune finalità specifiche o per trattare dati particolari in caso di sue specifiche richieste.

La comunicazione di dati a soggetti esterni (enti previdenziali e assicurativi, enti bilaterali, fondi di previdenza complementare, fondi di assistenza sanitaria integrativa, fondi interprofessionali di formazione continua, fondi contrattuali di formazione, pubbliche amministrazioni, organizzazioni sindacali, RSPP, RLS, RLST, OPT, medico del lavoro, eccetera) viene effettuata esclusivamente in adempimento alle normative vigenti ed alle disposizioni della contrattazione collettiva.

I dati personali sono conservati per tutta la durata del rapporto di lavoro, e anche successivamente secondo quanto previsto dalle norme vigenti.

La normativa sulla protezione dei dati le riconosce alcuni diritti (diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione) se ed in quanto applicabili (articoli da 15 a 22 del Regolamento UE n. 679 del 2016). Può inoltre proporre reclamo all'autorità di controllo, secondo le procedure previste dalla normativa vigente.

Per qualsiasi ulteriore informazione, e per far valere i diritti a lei riconosciuti dal Regolamento europeo, potrà rivolgersi a:

***Titolare del trattamento** (nome e cognome o denominazione in caso di ente o società): _____ (dati di contatto) _____*

***Responsabile della protezione dei dati - DPO** (nel caso sia stato nominato): (nome e cognome) _____ (dati di contatto) _____*

4.6 conferimento incarico ad effettuare operazioni di trattamento

Il modello che segue, opportunamente verificato ed integrato, può essere utilizzato per conferire l'incarico ai propri dipendenti, collaboratori, eccetera, ad effettuare operazioni di trattamento di dati personali di clienti, lavoratori, fornitori, eccetera.

Le informazioni inserite nel facsimile sono riportate a mero titolo esemplificativo. Ciascuna azienda è tenuta a riportare le informazioni corrette, integrando i dati mancanti.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Il sottoscritto ……Titolare / Responsabile dei trattamenti di dati personali, incarica il Sig. …….. ad effettuare le operazioni di trattamento dei dati personali connesse con la mansione affidata all'atto dell'assunzione e/o successivamente, necessarie per il normale svolgimento dell'attività aziendale.

Più in particolare, autorizza le seguenti operazioni:

- *registrazione e notifica alla Questura delle generalità dei clienti alloggiati, rilevate dai documenti di riconoscimento da loro esibiti, in adempimento della normativa di polizia vigente (art. 109 Testo Unico delle leggi di polizia)*
- *registrazione dei dati dei clienti per espletare la funzione di ricevimento e per inoltrare messaggi e telefonate*
- *registrazione dei dati necessari all'adempimento degli obblighi contabili e fiscali*
- *……..*
- *……..*
- *……..*

Per tali operazioni, da effettuare con correttezza e lecitamente, e secondo le istruzioni fornite, l'incaricato si avvarrà dell'ausilio di strumenti elettronici, e pertanto viene conferito il seguente CODICE IDENTIFICATIVO PERSONALE …….. e la seguente PASSWORD …… L'incaricato dovrà modificare la password al primo utilizzo e successivamente almeno ogni sei mesi.

La password, una volta modificata, dovrà essere comunicata al Sig. ……., incaricato della custodia delle copie delle credenziali di autenticazione. La password potrà essere utilizzata dal sottoscritto o dal Custode delle credenziali di autenticazione solo in caso di assenza dell'incaricato, che sarà comunque tempestivamente informato degli interventi effettuati.

L'incaricato non deve lasciare incustodito e accessibile a terzi lo strumento elettronico durante una sessione del trattamento.

Data

Firma del sottoscritto

Firma dell'incaricato per ricevuta

4.7 conferimento incarico di custode delle copie delle credenziali di autenticazione

Il modello che segue, opportunamente verificato ed integrato, può essere utilizzato per conferire ad un soggetto l'incarico di custodire copia delle credenziali di autenticazione (codice identificativo personale e password) assegnate ai lavoratori incaricati del trattamento di dati personali.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Il sottoscritto …….. Titolare / Responsabile dei trattamenti di dati personali, conferisce al Sig. …….. l'incarico di custodire le copie delle credenziali di autenticazione assegnate ai soggetti incaricati di trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici.

Le credenziali di autenticazione appartenenti ad un incaricato potranno essere utilizzate solo in caso di sua assenza. L'incaricato dovrà comunque essere tempestivamente informato degli interventi effettuati.

Data

Firma del sottoscritto

Firma dell'incaricato per ricevuta

4.8 attribuzione delle funzioni di amministratore di sistema

Riportiamo di seguito un modello per l'eventuale nomina dell'amministratore di sistema, da modificare ed integrare in relazione agli ambiti di operatività ed alle funzioni effettivamente svolte.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Il sottoscritto …….. Titolare dei trattamenti di dati personali, considerando la sua esperienza, capacità e affidabilità, le conferisce la funzione di amministratore di sistema (AdS) nei seguenti ambiti di operatività:

- *gestione del sistema operativo;*
- *gestione delle credenziali di autenticazione;*
- *gestione del data base;*
- *gestione delle reti;*
- *gestione degli strumenti e apparati di sicurezza;*
- *manutenzione hardware.*

Nello svolgimento della funzione di AdS dovrà rispettare le vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza nonché le istruzioni impartite dal titolare o dal responsabile.

Le ricordiamo:

- *che il suo operato sarà sottoposto a verifica da parte del Titolare o del Responsabile;*
- *che, a tal fine, saranno adottati sistemi per la registrazione degli accessi logici (autenticazioni informatiche);*
- *che i suoi estremi identificativi saranno riportati in un documento interno, disponibile in caso di accertamento da parte del Garante della protezione dei dati personali, e, nel caso in cui le sue mansioni riguardino anche indirettamente sistemi che permettano il trattamento di informazioni dei lavoratori, verranno resi conoscibili ai lavoratori medesimi;*
- *che l'attribuzione della funzione di AdS cessa in caso di attribuzione ad altro incarico che non preveda le attuali funzioni ovvero in caso di cessazione del suo rapporto di lavoro con l'azienda.*

Data

Firma del Titolare

Firma dell'incaricato per ricevuta

.

4.9 disciplinare aziendale in materia di utilizzo degli strumenti informatici

Il modello che segue, opportunamente modificato ed integrato, può essere utilizzato per informare i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica in azienda, e sulla possibilità che vengano effettuati controlli, come prescritto dall'Autorità Garante per la protezione dei dati personali[20].

Le informazioni inserite nel facsimile sono riportate a mero titolo esemplificativo. Ciascuna azienda è tenuta a riportare le informazioni corrette, apportando le modifiche necessarie e integrando le parti mancanti.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Gentile Signora/Signor ……

la informiamo che gli strumenti che le vengono dati in uso per espletare la sua attività lavorativa (rete internet accessibile da postazione client e servizio di posta elettronica) devono essere utilizzati con diligenza e correttezza, comportamenti che il lavoratore è sempre tenuto ad adottare nell'ambito del rapporto di lavoro.

Ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diverso rispetto alle finalità strettamente professionali deve essere limitato e occasionale. Poiché alcuni comportamenti possono mettere a rischio la sicurezza e l'immagine aziendale, anche nella normale attività lavorativa, di seguito vengono richiamate semplici regole procedurali finalizzate ad evitare condotte che inconsapevolmente possano causare rischi alla sicurezza del trattamento dei dati aziendali.

1. Posta Elettronica *- Il servizio di posta elettronica aziendale è disponibile per ogni lavoratore in forma centralizzata e protetta.*

Tale servizio è fruibile mediante specifico software client sia dall'Intranet che da Internet; è comunque possibile accedere via web alla casella personale.

Il servizio di posta elettronica aziendale non è un servizio in tempo reale, ovvero il tempo fra invio e ricezione di un messaggio non è istantaneo e dipende da molti fattori esterni.

L'invio di e-mail con allegati pesanti a mittenti multipli deve essere limitata onde evitare sovraccarico sul server centrale e sulle linee esterne.

In osservanza dei principi di pertinenza e non eccedenza, si adottano le seguenti misure di tipo organizzativo/tecnologico:

- *messa a disposizione di un indirizzo di posta elettronica condiviso per ufficio e/o servizio (ad esempio: segreteria@----------.it; helpdesk@----------it);*
- *attribuzione di un diverso indirizzo di posta elettronica destinato ad uso esclusivo del lavoratore;*
- *messa a disposizione di ciascun lavoratore di apposite funzionalità di sistema che consentono di inviare automaticamente, in caso di assenze programmate, messaggi*

[20] Provvedimento n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007 - doc. web n. 1387522. Vedi punto 2.2.

di risposta che contengano le coordinate di un altro soggetto o altre utili modalità di contatto presso l'azienda;

- *messa a disposizione di sistemi che consentono al lavoratore di delegare un collega a verificare il contenuto dei suoi messaggi e ad inoltrare quelli significativi per l'attività lavorativa, in caso di assenza improvvisa o prolungata del lavoratore;*
- *graduazione dei controlli che avverranno secondo le modalità di seguito indicate.*

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. Il rispetto di alcune semplici regole può aiutare a migliorare ulteriormente l'utilizzo dello strumento. La casella di posta elettronica aziendale personale deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.

È possibile utilizzare la ricevuta di ritorno per avere la conferma della avvenuta lettura del messaggio da parte del destinatario.

L'utilizzo degli strumenti di comunicazione telematici deve necessariamente fare riferimento alle procedure in essere per quanto attiene alla verifica e circolazione delle comunicazioni prodotte o ricevute. In generale ogni comunicazione, inviata o ricevuta che abbia contenuti significativi o contenga impegni contrattuali o precontrattuali per l'azienda, deve essere visionata e autorizzata dal titolare dell'azienda o dal responsabile del servizio, o comunque deve essere rispettata la procedura in essere per la corrispondenza ordinaria.

È fatto divieto di utilizzare la casella di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed espressa autorizzazione da parte del titolare dell'azienda o del responsabile del servizio.

È in facoltà del lavoratore avere un proprio indirizzo elettronico presso sistemi esterni web; l'utilizzo di tale posta elettronica privata è consentito entro tollerabili limiti temporali.

È da evitare la divulgazione degli indirizzi destinati alla ricezione di comunicazioni ufficiali. In caso di ricezione accidentale di messaggi di valenza ufficiale sulle caselle assegnate, gli assegnatari riceventi dovranno inoltrarli tempestivamente al titolare dell'azienda o al responsabile del servizio.

2. Antivirus *- Tutti i computer aziendali (Client e P.C. portatili) sono protetti da apposito software che:*

- *protegge in tempo reale il computer e i dati letti/scritti;*
- *può verificare che tutte le informazioni presenti nei dischi siano libere da virus;*
- *aggiorna automaticamente il dizionario dei virus; questa attività viene eseguita ad ogni collegamento alla Intranet aziendale;*
- *gestisce e rende visibile centralmente lo stato dei computer;*
- *distribuisce gli aggiornamenti mediante i server di sede.*

3. Utilizzo dell'elaboratore e della rete interna *- L'accesso all'elaboratore, sia esso in rete o "stand alone", è sempre protetto da una o più password.*

La password deve essere composta da almeno n. 8 (otto) caratteri alfanumerici, oppure, nel caso in cui lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'incaricato (nome o data di nascita propri o dei propri familiari, nome del proprio cane o altri elementi simili) ed è modificata da quest'ultimo al primo utilizzo e, successivamente,

almeno ogni sei mesi (tre mesi in caso di trattamento di dati sensibili). Le password assegnate sono personali e non devono essere divulgate a terzi, fatta eccezione per il custode delle credenziali di autenticazione incaricato dall'azienda, e devono essere custodite dall'assegnatario con la massima diligenza.

Il lavoratore ha altresì l'obbligo di comunicare la password adottata ad ogni sua variazione, in busta chiusa firmata e datata di suo pugno, al custode delle credenziali di autenticazione incaricato dall'azienda. Il titolare dell'azienda o il responsabile del servizio, in caso di emergenza e/o di assenza del lavoratore, hanno il diritto di accedere al suo computer ed ai contenuti ivi custoditi per esigenze di carattere lavorativo, utilizzando la password comunicata al custode delle credenziali di autenticazione, e dando successiva comunicazione dell'avvenuto accesso al lavoratore.

Possono essere introdotte limitazioni all'accesso agli archivi aziendali, laddove il titolare dell'azienda o il responsabile del servizio lo ritengano opportuno.

È tassativamente proibito installare programmi provenienti dall'esterno, in quanto l'utilizzo di software non regolarmente acquistato dall'azienda può configurare un reato, anche in considerazione del grave pericolo di contrarre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Le unità di rete sono aree di condivisione di informazioni strettamente aziendali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte del titolare o persona da questi designata, che possono, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterranno pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui PC dei lavoratori sia sulle unità di rete.

Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici e comunque protetto nelle pause durante l'orario di lavoro.

Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Tutti i supporti magnetici riutilizzabili (cd, dischetti, pendrive) contenenti dati personali devono essere trattati con particolare cautela. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione. Per questo motivo il supporto, al termine dell'utilizzo, deve essere formattato prima di essere riutilizzato oppure distrutto.

Il lavoratore avrà cura di effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla immediatamente dai vassoi delle stampanti comuni. Si eviterà in ogni modo e per quanto possibile, di dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (per esempio: corridoi, sale d'attesa, ecc.).

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti direttive, sotto la sorveglianza del titolare del trattamento dei dati personali o persona da questi designata.

4. Utilizzo della rete internet e dei relativi servizi *- L'utilizzo imprudente di alcuni servizi della rete Internet, ancorché nell'ambito della normale attività aziendale, può essere fonte di particolari minacce alla sicurezza dei dati e all'immagine aziendale.*

Seguono alcune semplici regole che devono essere osservate in tale circostanza.

Dall'interno della rete aziendale:

- *è da evitare lo scaricamento (upload e/o download) di file e/o programmi software, anche gratuiti, se non per esigenze strettamente aziendali e fatti comunque salvi i casi di esplicita autorizzazione del titolare dell'azienda o del responsabile del servizio;*
- *è tassativamente proibita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal titolare dell'azienda o dal responsabile del servizio e con il rispetto delle normali procedure per gli acquisti;*
- *è vietata la partecipazione a forum non aziendali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività aziendale;*
- *è vietato l'uso della rete per accessi a servizi con finalità ludiche o estranei all'attività per tempi eccessivamente prolungati e comunque durante l'orario di servizio.*

5. Controlli e conservazione dei dati *- Il titolare ha predisposto il proprio sistema informativo e la rete intranet ed internet al fine di utilizzare tali beni aziendali per esclusive esigenze organizzative e/o produttive.*

A tal fine, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori, di sistemi che consentono indirettamente un controllo a distanza (controlli preterintenzionali) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori; e ciò, anche in presenza di attività di controllo discontinue.

In particolare, tale attività di controllo potrà essere esercitata nel caso in cui si rivelino anomalie di funzionamento o si rendano necessarie attività di manutenzione o, comunque, in tutte le ipotesi in cui sia a rischio la sicurezza dei citati beni aziendali e/o la sicurezza sul lavoro in generale.

Questa attività di controllo a distanza sarà pertanto lecita e dettata dal principio di necessità. Il titolare dichiara di non utilizzare sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

- *la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;*
- *la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;*
- *la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo;*
- *l'analisi occulta dei computer portatili affidati in uso.*

Il titolare si riserva:

- *di effettuare controlli a campione, nel rispetto dei principi di pertinenza e non eccedenza, secondo le prescrizioni contenute nel presente disciplinare;*
- *di verificare comportamenti anomali, anche individuali, nel caso in cui un evento dannoso e/o una situazione di pericolo non siano stati impediti con i preventivi accorgimenti tecnici standard;*
- *di effettuare i controlli individuali su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree;*
- *di effettuare controlli anonimi causati da un rilevato utilizzo anomalo degli strumenti aziendali il cui esito deve essere comunicato tramite avviso generalizzato.*

Il titolare esclude la possibilità di effettuare controlli prolungati, costanti e/o indiscriminati.

In merito alla conservazione dei dati, il titolare adotta sistemi software programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica e comprovata e limitata nel tempo necessario a raggiungerla.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:

- *ad esigenze tecniche o di sicurezza del tutto particolari;*
- *all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;*
- *all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria. In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.*

6. PC Portatili *- L'azienda consegna ad alcuni lavoratori i PC portatili, il cui utilizzo deve essere autorizzato dal titolare o dal responsabile del servizio. Le regole di utilizzo di queste apparecchiature sono le medesime indicate per i PC connessi alla rete.*

I portatili che vengono sconnessi dalla rete aziendale e restano per lunghi periodi fuori dall'intranet, non ricevono gli aggiornamenti automatici e pertanto hanno un grado di protezione non allineato con gli standard aziendali.

7. Attività di formazione *- L'azienda predispone regolari momenti formativi e informativi per garantire a tutti i lavoratori incaricati il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.*

4.10 informativa ai fornitori

Il modello di informativa che segue, da modificare e integrare a seconda delle specifiche esigenze, va consegnato ai fornitori (se persone fisiche quali ditte individuali, società di persone, professionisti, eccetera) o reso loro disponibile.

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

Ai sensi della normativa vigente in materia di protezione dei dati (Regolamento (UE) 2016/679 - D. Legisl. 196/2003), desideriamo informarla che i trattamenti dei suoi dati personali sono effettuati con correttezza e trasparenza, per fini leciti e tutelando la sua riservatezza ed i suoi diritti.

I trattamenti sono effettuati, anche con l'ausilio di mezzi informatici, in esecuzione di di misure precontrattuali e di contratto, e per adempiere ai vigenti obblighi amministrativi, contabili e fiscali. Per tali finalità il trattamento è effettuato senza necessità di acquisire il suo consenso.

I dati sono trattati da noi e da nostri responsabili e incaricati, e vengono comunicati all'esterno solo in adempimento ad obblighi di legge. I dati acquisiti per tali finalità vengono da noi conservati per il tempo previsto dalle rispettive normative (10 anni, e anche oltre in caso di contenzioso o accertamenti fiscali).

La normativa vigente le riconosce alcuni diritti (diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione) se ed in quanto applicabili (articoli da 15 a 22 del Regolamento UE n. 679 del 2016). Può inoltre proporre reclamo all'autorità di controllo, secondo le procedure previste dalla normativa vigente.

Per qualsiasi ulteriore informazione, e per far valere i diritti a lei riconosciuti dal Regolamento europeo, potrà rivolgersi a:

***Titolare del trattamento** (nome e cognome o denominazione in caso di ente o società): _____ (dati di contatto) _____*

***Responsabile della protezione dei dati - DPO** (nel caso sia stato nominato): (nome e cognome) _____ (dati di contatto) _____*

4.11 registro dei trattamenti di dati

Il Garante ha reso disponibile un modello di "registro semplificato" delle attività di trattamento del titolare e del responsabile, realizzato per le piccole e medie imprese (https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento).

Abbiamo provveduto a integrare il modello reso disponibile dal Garante, tenendo conto dei trattamenti tipici delle strutture ricettive, riportando informazioni e dati a mero titolo esemplificativo.

Ciascuna azienda è tenuta a riportare le informazioni corrette, eventualmente scegliendo tra le diverse opzioni e integrando i dati mancanti[21].

Il modello potrà subire modifiche o integrazioni in caso di emanazione da parte del Garante di specifici chiarimenti su aspetti di coordinamento tra la normativa nazionale ed il Regolamento europeo.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
ATTENZIONE: LE INFORMAZIONI E I DATI INSERITI NELLE TABELLE SONO RIPORTATI A MERO TITOLO ESEMPLIFICATIVO. **CIASCUNA AZIENDA È TENUTA A RIPORTARE LE INFORMAZIONI CORRETTE, EVENTUALMENTE SCEGLIENDO TRA LE DIVERSE OPZIONI E INTEGRANDO I DATI MANCANTI.**
SCHEDA REGISTRO DEI TRATTAMENTI per i contenuti vedi Faq sul registro delle attività di trattamento https://www.garanteprivacy.it/regolamentoue/registro
DENOMINAZIONE DELLA STRUTTURA RICETTIVA
RAGIONE SOCIALE
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE (inserire la denominazione e i dati di contatto)
RESPONSABILE DELLA PROTEZIONE DEI DATI (inserire la denominazione e i dati di contatto, se nominato)

[21] Relativamente ai soggetti obbligati alla tenuta del registro, e ai dati che è necessario riportare, vedi il punto 1.13. Ricordiamo che la tenuta del Registro è fortemente raccomandata dal Garante anche nei casi in cui non sia obbligatoria.

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE PER LA GENERALITA' DEI TRATTAMENTI	**Descrizione degli strumenti utilizzati**: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. **Tipologia di dispositivi di accesso**: pc n.____. **Tipologia di interconnessione**: Rete locale LAN. **Comportamento degli operatori incaricati**: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione. **Rischi di furto di credenziali di autenticazione (password e user-id)**: l'accesso alla struttura ricettiva, e dunque agli elaboratori ed al database, è continuamente sorvegliato e quindi è altamente improbabile che l'eventuale sottrazione delle credenziali di autenticazione possa procurare esiti dannosi. Il sistema, comunque, mantiene traccia degli accessi praticati allo scopo di accertare eventuali comportamenti illegittimi. Rischio basso. **Rischi da carenza di consapevolezza, disattenzione o incuria**: La consapevolezza del personale, conseguente al livello professionale dello stesso ed alle disposizioni adottate in materia di protezione dei dati, rende altamente improbabile comportamenti di disattenzione o incuria da parte dei dipendenti. Rischio basso. **Rischi di comportamenti sleali o fraudolenti**: L'obbligo di lealtà implicito nei rapporti di lavoro rende mediamente improbabile comportamenti sleali e fraudolenti finalizzati ad un uso improprio dei dati. Rischio medio. **Rischi di errori materiali**: L'utilizzo di procedure automatizzate e la competenza e professionalità dei lavoratori rendono mediamente improbabile il verificarsi di errori materiali. Rischio medio. **Rischi da azione di virus informatici o di codici malefici**: Il sistema è protetto da un dispositivo Firewall che aggiorna anche periodicamente i pattern di verifica antivirus. Su ogni stazione è installato il relativo filtro antivirus. Nel caso in cui dovesse comunque verificarsi l'evento, gli archivi possono essere immediatamente ripristinati poiché viene effettuato backup giornaliero in duplice copia degli archivi stessi. Rischio basso. **Rischi da spamming o altre tecniche di sabotaggio**: Il dispositivo Firewall protegge anche da programmi in grado di generare in seguito spamming. Rischio basso. **Rischi da malfunzionamento, indisponibilità o degrado degli strumenti**: Il controllo sullo stato dell'hardware è costante e le eventuali operazioni di ripristino possono essere effettuate in tempi brevi. Guasti e malfunzionamenti non possono però essere completamente esclusi. Rischio basso. **Rischi da accessi esterni non autorizzati**: Attraverso Internet l'accesso è impedito dal dispositivo Firewall. Rischio basso. **Rischi da intercettazione di informazioni in rete**: I dati sono protetti da password. Rischio basso. **Rischi da accessi non autorizzati a locali/reparti ad accesso ristretto; asportazione e furto di strumenti contenenti dati**: L'accesso alla struttura ricettiva è continuamente presidiato. Rischio basso. **Rischi da eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria**: Tali eventi non possono essere totalmente esclusi, anche se la struttura è tenuta al rispetto di precise regole di sicurezza e prevenzione incendi. Le eventuali operazioni di ripristino possono essere però effettuate in tempi brevi. Rischio basso. **Rischi da guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)**: L'impianto elettrico è costantemente manutenuto ed è presente il gruppo di continuità. Rischio basso. **Rischi da errori umani nella gestione della sicurezza fisica**: Il personale è adeguatamente formato in ordine alla prevenzione di rischi. Rischio basso.

TIPOLOGIA DI TRATTAMENTO	**FINALITÀ E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERESSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI (indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati)**	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI (indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del GDPR)**	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE SPECIFICHE**
TRATTAMENTO DEI DATI DI LAVORATORI E COLLABORATORI PER LA GESTIONE DEL RAPPORTO DI LAVORO	ADEMPIMENTO DEGLI OBBLIGHI AMMINISTRATIVI, RETRIBUTIVI, CONTRIBUTIVI, FISCALI, DI SICUREZZA SUL LAVORO - Obblighi di legge - Richiesta di consenso per l'eventuale trattamento di dati particolari idonei a rivelare lo stato di salute o le convinzioni politiche, religiose o di altro genere, o l'adesione ad associazioni o sindacati, trattati al solo fine di adempiere agli obblighi derivanti dalle normative vigenti o dalle disposizioni della contrattazione collettiva, o in adempimento di specifiche richieste dello stesso interessato.	Lavoratori, Collaboratori	Dati personali attinenti alla retribuzione, a rimborsi spese, al pagamento di imposte e contributi	Enti previdenziali e assicurativi, enti bilaterali, fondi di previdenza complementare, fondi di assistenza sanitaria integrativa, fondi interprofessionali di formazione continua, fondi contrattuali di formazione, pubbliche amministrazioni, eccetera	No/Si	Termini di legge (5/10 anni, anche oltre in caso di contenzioso)	Descrizione degli strumenti utilizzati: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. Tipologia di dispositivi di accesso: pc n.____. Tipologia di interconnessione: Rete locale LAN. Operatori incaricati: Ufficio del personale - Ufficio amministrazione - Collaboratori esterni incaricati degli adempimenti amministrativi, retributivi, contributivi, fiscali e di sicurezza sul lavoro - Medico del lavoro. Comportamento degli operatori incaricati: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione.

TRATTAMENTO DI DATI PERSONALI DEI FORNITORI	ADEMPIMENTO DEGLI OBBLIGHI AMMINISTRATIVI E FISCALI - Obblighi di legge e adempimenti contrattuali	Fornitori di prodotti e servizi	Generalità e recapiti Codice fiscale e/o partita iva Dati bancari	Agenzia delle entrate Studio commercialista ……. Collaboratori esterni incaricati degli adempimenti amministrativi e fiscali	No/Si	Termini di legge (10 anni ai sensi dell'articolo 2220 del codice civile e anche oltre in caso di contenzioso)	Descrizione degli strumenti utilizzati: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. Tipologia di dispositivi di accesso: pc n.____. Tipologia di interconnessione: Rete locale LAN. Operatori incaricati: Ufficio amministrazione - Collaboratori esterni incaricati degli adempimenti amministrativi e fiscali. Comportamento degli operatori incaricati: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione.
TRATTAMENTO DI DATI PERSONALI DI CLIENTI E OSPITI	PRENOTAZIONE DEL SERVIZIO DI ALLOGGIO E DI SERVIZI ACCESSORI - FORNITURA DEL SERVIZIO DI ALLOGGIO E SERVIZI ACCESSORI - PAGAMENTO DEI CORRISPETTIVI E ADEMPIMENTI CONNESSI - Misure precontrattuali, adempimenti contrattuali, obblighi di legge, consenso, se non ricorrono le condizioni di cui sopra	Clienti e ospiti	Generalità e recapiti Codice fiscale e/o partita iva Estremi carte di credito e debito forniti a garanzia e/o a saldo	Agenzia delle entrate Studio commercialista …. Collaboratori esterni incaricati degli adempimenti amministrativi e fiscali Circuiti bancari e carte di credito	No/Si	Termini di legge, se in adempimento di obblighi di legge (10 anni ai sensi dell'articolo 2220 del codice civile e anche oltre in caso di contenzioso) …….mesi/anni, se il trattamento è basato sul consenso	Descrizione degli strumenti utilizzati: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. Tipologia di dispositivi di accesso: pc n.____.

							Tipologia di interconnessione: Rete locale LAN. Operatori incaricati: Ufficio prenotazioni - Addetti al ricevimento - Ufficio amministrazione - Collaboratori esterni incaricati degli adempimenti amministrativi e fiscali. Comportamento degli operatori incaricati: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione.
TRATTAMENTO DI DATI PERSONALI DI CLIENTI E OSPITI	NOTIFICA ALLA QUESTURA DEI DATI DEGLI ALLOGGIATI - obbligo di legge ex articolo 109 TULPS	Clienti alloggiati	Generalità ed estremi dei documenti di riconosciment o Notti di pernottamento Relazioni di parentela	Questura	No	Cancellazione dopo l'invio e conservazione delle ricevute digitali di invio per 5 anni Conservazione per ……. mesi/anni previa acquisizione del consenso dell'interessato	Descrizione degli strumenti utilizzati: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____ _____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. Tipologia di dispositivi di accesso: pc n.____. Tipologia di interconnessione: Rete locale LAN. Operatori incaricati: Addetti al ricevimento – Segreteria. Comportamento degli operatori incaricati: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di

							protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione.
TRATTAMENTO DI DATI PERSONALI DI CLIENTI E OSPITI	ATTIVITÀ DI MARKETING E FIDELIZZAZIONE DEI CLIENTI - acquisizione del consenso	Clienti e potenziali clienti	Generalità ed indirizzi postali e/o elettronici		No/Si	Indirizzi postali e/o elettronici: …..anni	Descrizione degli strumenti utilizzati: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____ _____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. Tipologia di dispositivi di accesso: pc n.____. Tipologia di interconnessione: Rete locale LAN. Operatori incaricati: Ufficio marketing – Segreteria. Comportamento degli operatori incaricati: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione.

TRATTAMENTO DI DATI PERSONALI DI CLIENTI, OSPITI, LAVORATORI E COLLABORATORI	VIDEOSORVEGLIANZA AI FINI DI PROTEZIONE DELLE PERSONE, DELLA PROPRIETÀ E DEL PATRIMONIO AZIENDALE - perseguimento di un legittimo interesse del titolare, per fini di tutela delle persone e dei beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e per finalità di prevenzione incendi e di sicurezza del lavoro	Clienti, ospiti, lavoratori e collaboratori	Immagini		No/Si	24 ore, salvo festivi o altri casi di chiusura dell'esercizio, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria, e comunque non oltre una settimana	Descrizione degli strumenti utilizzati: Data base applicazione Windows. Ubicazione fisica dei supporti di memorizzazione: Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo_____ _____. Memorizzazione su cloud di cloud provider con sede in Europa / Extra UE. Tipologia di dispositivi di accesso: pc n.____. Tipologia di interconnessione: Rete locale LAN. Operatori incaricati: Addetti al ricevimento – Portineria - Addetti alla sicurezza. Comportamento degli operatori incaricati: Agli operatori che procedono alla acquisizione, caricamento e consultazione di dati personali sono fornite specifiche istruzioni in materia di protezione dei dati. La comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati. Nell'accesso agli strumenti informatici gli incaricati utilizzano credenziali di autenticazione.
TRATTAMENTO DI DATI PERSONALI DI …… ……..							
REGISTRO CREATO IN DATA…….							
ULTIMO AGGIORNAMENTO AVVENUTO IN DATA ……							

Federalberghi offre ai propri soci

una tutela a 360° che comprende rappresentanza istituzionale, relazioni sindacali, consulenza, informazione, opportunità di business, convenzioni per ottenere sconti e agevolazioni, finanziamenti per la formazione, studi e ricerche, sicurezza sul lavoro, assistenza sanitaria, previdenza complementare ... e tanto altro.

www.confturismo.it

www.confcommercio.it

www.hotrec.org

www.ebnt.it

www.federalberghi.it

www.hotelmag.it

www.turismoditalia.it

www.italyhotels.it

www.hotelstars.eu

www.buonivacanze.it

www.10q.it

www.siaguest.it

www.federalberghi.it

www.conventionbureau.com

www.icctalia.org

www.adapt.it

www.fondoforte.it

www.cfmt.it

www.fondir.it

www.unibocconi.it/met

www.consorzioconoe.it

www.federalberghi.it

www.fondofast.it

www.quas.it

www.fasdac.it

www.fondofonte.it

www.fondomarionegri.it

www.fondomariopastore.it

www.scfitalia.it

www.siae.it

www.zurich.it

www.unilever.it

www.reshbd.com

www.grohe.it

www.nuovoimaie.it

www.assobiomedica.it

www.unicredit.it

www.mcwatt.it

www.unogas.it

www.hoistgroup.com

www.verticalbooking.com

Vuoi saperne di più sul sistema Federalberghi?

Rivolgiti con fiducia ad una delle 145 associazioni territoriali e regionali degli albergatori aderenti a Federalberghi.

I recapiti sono disponibili sul sito www.federalberghi.it

Le guide degli alberghi

Ista, istituto di studi alberghieri intitolato a Giovanni Colombo, compianto presidente di Federalberghi, elabora analisi, indagini e ricerche sui temi di principale interesse per la categoria, autonomamente e in partnership con prestigiosi Istituti di ricerca.

La protezione dei dati personali nella gestione delle imprese ricettive, 2019
Ecobonus: istruzioni per l'uso, 2019
Come ripensare la ristorazione, per soddisfare le nuove esigenze dell'ospite, 2018
La reception per tutti, 2018
Incentivi sulla riqualificazione delle strutture ricettive, 2015 - 2018
Direct booking, 2017
L'albergo (manuale della collana Le Bussole), 2017
Alternare formazione e lavoro. Il progetto scuola, 2017-2018
Nuova disciplina delle prestazioni occasionali, 2017
Sommerso turistico ed affitti brevi, 2016
Locazioni brevi e sharing economy, 2016
Indagine sulle tourist card, 2016
Datatur, trend e statistiche sull'economia del turismo, 2016
L'apporto di Federalberghi al Decreto Turismo, 2016
Seminario istituzionale sul regime fiscale delle locazioni brevi, 2015
La privacy nell'ospitalità, 2002 - 2015
Taccuino degli allergeni, 2015
Osservatorio sul mercato del lavoro nel settore turismo, 2015
L'antitrust sanziona Tripadvisor, 2015
Stop all'abusivismo, 2014 - 2015
L'imposta di soggiorno. Osservatorio sulla fiscalità locale, 2012 - 2015
Datatur, trend e statistiche sull'economia del turismo, 2015
Ospitare, servire, ristorare. Storia dei lavoratori di alberghi e ristoranti in Italia dalla fine dell'Ottocento alla metà del Novecento, 2014
Settimo rapporto sul sistema alberghiero italiano, 2014
L'appalto di servizi nelle aziende alberghiere, 2009 - 2014
@Hotel: digital marketing operations, 2014
L'alternanza scuola-lavoro nel settore turismo, 2014
I contratti a termine nel settore turismo dopo il jobs act, 2014
Il lavoro intermittente nel settore turismo, 2006 - 2014
Datatur, trend e statistiche sull'economia del turismo, 2014
I tirocini formativi nel settore turismo, 2014
Agevolazioni fiscali sul gas naturale, 2014
Federalberghi ricorre all'Antitrust contro le on line travel agencies, 2014 - 2015
Guida al nuovo CCNL Turismo, 2014

Riflessioni e proposte per il rinnovo del CCNL Turismo, 2013
Datatur, trend e statistiche sull'economia del turismo, 2013
Osservatorio sul mercato del lavoro nel settore turismo, 2012
Il lavoro delle donne nel settore turismo, 2012
Percorsi formativi in Italia per il settore turismo, 2012
La successione dei contratti a termine nel settore turismo, 2012
Datatur, trend e statistiche sull'economia del turismo, 2012
Il turismo lavora per l'Italia, 2012
Il lavoro accessorio nel Turismo, 2009 - 2011
La contrattazione di secondo livello nel settore turismo, 2011
Misure per l'incremento della produttività del lavoro, 2011
Gli stage nel settore turismo - ed. speciale progetto RE.LA.R., 2011
Gli stage nel settore turismo, 2004 - 2011
L'apprendistato stagionale dopo la riforma, 2011
La sicurezza antincendio negli alberghi italiani, 2011
Metodologia di sicurezza antincendio MBS, 2011
Imposta municipale unica, 2011
Guida al mercato russo, 2011
Datatur, trend e statistiche sull'economia del turismo, 2011
Il lavoro intermittente nel Turismo, 2009 – 2010
Guida al nuovo CCNL Turismo, 2010
L'apprendistato nel settore Turismo, 2010
Sesto rapporto sul sistema alberghiero, 2010
Indagine sui fabbisogni formativi nel settore Turismo, 2010
Agevolazioni fiscali sul gas naturale, 2010
Osservatorio sul mercato del lavoro nel settore turismo, 2009
La pulizia professionale delle camere albergo, 2009
Gli ammortizzatori sociali nel settore Turismo, 2009
Il contratto di inserimento nel settore Turismo, 2009
Internet e Turismo, 2009
Guida al nuovo CCNL Turismo, 2007
Quinto rapporto sul sistema alberghiero, 2007
Mercato del lavoro e professioni nel settore Turismo, 2006
Come cambia il lavoro nel Turismo, 2006
Incentivi per le imprese nelle aree sottoutilizzate, 2006
Quarto rapporto sul sistema alberghiero, 2005
Il pronto soccorso nel settore Turismo, 2005
Dimensione dell'azienda turistica e agevolazioni pubbliche, 2005
La nuova disciplina del lavoro extra, 2004 - 2010
Dati essenziali sul movimento turistico, 2004
Dati essenziali sul movimento turistico nazionale ed internazionale, 2004
I contratti part time nel settore Turismo, 2004
I tirocini formativi nel settore Turismo, 2004

I condoni fiscali, 2003
Mercato del lavoro e professioni nel settore turismo, 2003
Repertorio dei percorsi formativi universitari per il settore turismo, 2003
Le attività di intrattenimento negli alberghi, 2003
La riforma dell'orario di lavoro, 2003
La riforma del part time, 2003
Terzo rapporto sul sistema alberghiero in Italia, 2002
I congedi parentali, 2002
Il turismo religioso in Italia, 2002
Il nuovo contratto di lavoro a termine, 2001 - 2002
Il nuovo collocamento dei disabili , 2001
Le stagioni dello sviluppo, 2001
Sistema ricettivo termale in Italia, 2001
Indagine sulla domanda turistica nei paesi esteri, 2001
Sistema ricettivo delle località termali in Italia, 2001
La flessibilità del mercato del lavoro, 2000
Osservatorio sulla fiscalità locale, 2000
Il Turismo lavora per l'Italia, 2000
Norme per il soggiorno degli stranieri, 2000
Indagine sulla domanda turistica nei paesi esteri, 2000
Secondo rapporto sul sistema alberghiero in Italia, 2000
Il codice del lavoro nel turismo, 1999 - 2003
Primo rapporto sul sistema alberghiero in Italia, 1999
Il collocamento obbligatorio, 1998
Manuale di corretta prassi igienica per la ristorazione, 1998
Diritti d'autore ed imposta spettacoli, 1997
La qualità e la certificazione ISO 9000 nell'azienda alberghiera, 1997
Il lavoro temporaneo, 1997
Analisi degli infortuni nel settore turismo, 1997
La prevenzione incendi negli alberghi: il registro dei controlli, 1996
La prevenzione incendi negli alberghi: come gestire la sicurezza, 1995
Il Turismo nelle politiche strutturali della UE, 1995
Il franchising nel settore alberghiero, 1995
Il finanziamento delle attività turistiche, 1994
Igiene e sanità negli alberghi, 1994
Linee guida per la costruzione di un modello di analisi del costo del lavoro, 1994
Costo e disciplina dei rapporti di lavoro negli alberghi dei Paesi CEE, 1993
Per una politica del turismo, 1993
Ecologia in albergo, 1993
Quale futuro per l'impresa alberghiera, 1993
La pulizia professionale delle camere d'albergo, 1993
Il turismo culturale in Italia, 1993
Il turismo marino in Italia, 1993

Serie storica dei minimi retributivi, 1993
Esame comparativo dei criteri di classificazione alberghiera, 1992
L’albergo impresa, 1990

Federalberghi da oltre cento anni è l'organizzazione nazionale maggiormente rappresentativa degli albergatori italiani.

La federazione rappresenta le esigenze e le proposte delle imprese alberghiere nei confronti delle istituzioni e delle organizzazioni politiche, economiche e sindacali.

Aderiscono a Federalberghi 127 associazioni territoriali e una delegazione territoriale, raggruppate in 19 unioni regionali, e 7 Sindacati Nazionali (Unione Nazionale Italiana Catene Alberghiere, Sindacato Grandi Alberghi, Sindacato Villaggi Turistici, Federalberghi Extra, Federalberghi Isole Minori, Federalberghi Terme, Unihotel Franchising).

L'associazione rappresenta gli interessi degli albergatori nei confronti delle istituzioni e delle organizzazioni sindacali.

Faiat service srl è il braccio operativo di Federalberghi.

Il Presidente è Bernabò Bocca.
Il Direttore Generale è Alessandro Massimo Nucara.

Federalberghi aderisce dal 1950 a Confcommercio ove, insieme alle principali federazioni di categoria che operano nel Turismo, ha dato vita a Confturismo, l'organizzazione di rappresentanza imprenditoriale di settore.

Federalberghi è socio fondatore di Hotrec, la Confederazione Europea degli imprenditori del settore alberghiero e della ristorazione.