Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

Data Protection: il Professionista del Trattamento e della Protezione dei Dati Personali

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

Tecnologia e normativa di riferimento sul controllo dei lavoratori

- Processi di Geolocalizzazione e di Identificazione (Biometrica)
- Videosorveglianza
- Controlli a distanza sul lavoratore: posta elettronica, navigazione internet e social network

CONTROLLI A DISTANZA SUL LAVORATORE

Controlli a distanza sul lavoratore

I diritti e i doveri del lavoratore

- L'articolo 2104 del codice civile ("**diligenza del prestatore di lavoro**") stabilisce che:

  - *"Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.*

  - *Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende".*

Controlli a distanza sul lavoratore

- Il controllo sui lavoratori
  - Articolo 4 Statuto dei Lavoratori
  - Natura giuridica della mail
- Obblighi di legge in tema di mantenimento di log
  - Art. 132 D.lgs. 196/03, così come emendato dal D.lgs. 101/2018
  - Provvedimento amministratori di sistema 27 novembre 2008
  - Provvedimento Garante 192/2011 (Banche)
  - Provvedimento Garante giugno 2015 (Dossier Sanitario)

Overview

Con le moderne tecnologie è possibile «tracciare» il lavoratore in ogni momento, sia al lavoro che nei suoi luoghi privati, utilizzando diversi device tra smartphone, pc, tablet, veicoli e device 'indossabili'.

Senza limiti e senza trasparenza, c'è un alto rischio che un legittimo interesse dell'azienda di incrementare la propria produttività si traduca in un **monitoraggio sul lavoratore sprovvisto di adeguate giustificazioni e garanzie**.

Overview

- Il monitoraggio tramite strumenti IT è molto meno visibile e i relativi tool possono agire senza che il lavoratore ne abbia chiara evidenza.
- Senza la previsione di policy a riguardo, il lavoratore non può essere edotto delle conseguenze del monitoraggio in atto, e non può quindi esercitarne i relativi diritti.
- Un alto rischio è dato anche dall'eccedenza nella raccolta di dati personali da parte di questi sistemi.

Overview

Tipologia di illecito:

- Illeciti che si configurano solo nel «non lavoro»
- Illeciti che si configurano nel «non lavoro» e nell'aggressione a un bene aziendale tutelato

Tipologia di controlli:

- Preventivi: controlli «orizzontali» mirati a prevenire illeciti in modo ampio e generalizzato
- Reattivi: quando conseguono all'emersione di elementi di fatto tali da raccomandare l'avvio di una indagine retrospettiva

Dubbi e domande ricorrenti

- Quali informazioni ci sono in azienda? Quali sono le fonti? Per quanto tempo sono conservate?
- Per quali motivi sono raccolte e mantenute?
- Quali informazioni posso raccogliere?
- Quali informazioni devo raccogliere?
- Per cosa posso usare le informazioni che vengono raccolte?
- Quali controlli preventivi possono essere posti in essere?
- Se dovessero servire le informazioni, come occorre acquisirle e mantenerle?

- Quali competenze occorre coinvolgere (tecniche - HR – relazioni industriali – legali)?
- Quali procedure e tempistiche prescrizionali occorre rispettare?
- Le informazioni presenti possono essere prodotte in sede processuale?
- Le informazioni presenti potranno essere considerate dal magistrato in sede processuale a fondamento di una decisione?
- Come occorre agire per raccogliere le evidenze digitali?
  - Garanzie per il lavoratore?
  - Metodologie?

Statuto dei lavoratori

Articolo 4 comma 1

Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.

In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

Statuto dei lavoratori

Articolo 4 commi 2 e 3

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

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

Chiarimenti del ministero

18 giugno 2015

Ministero del Lavoro: nessuna liberalizzazione, norma in linea con le indicazioni del Garante della Privacy

Non possono essere **considerati "strumenti di controllo a distanza" gli strumenti** che vengono assegnati al lavoratore "per rendere la prestazione lavorativa" (una volta si sarebbero chiamati gli "attrezzi di lavoro"), **come pc, tablet e cellulari**.

In tal modo, viene fugato ogni dubbio - per quanto teorico- circa la necessità del previo accordo sindacale anche per la consegna di tali strumenti.

Chiarimenti del ministero

L'espressione "per rendere la prestazione lavorativa" comporta che **l'accordo o l'autorizzazione non servono se**, e nella misura in cui, **lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione**: ciò significa che, *nel momento in cui tale strumento viene modificato* (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, *si fuoriesce dall'ambito della disposizione*: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che (*attraverso i quali è possibile*) servono al datore per controllarne la prestazione.

Con la conseguenza che queste "modifiche" possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione.

Perciò, è bene ribadirlo, **non si autorizza nessun controllo a distanza**; piuttosto, **si chiariscono solo le modalità** per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa ed i limiti di utilizzabilità dei dati raccolti con questi strumenti.

Privacy e Statuto dei lavoratori

Problematiche

- Possibilità di **violare diritti soggettivi dei dipendenti** (libertà di circolazione e comunicazione) attraverso **l'accesso ad informazioni ulteriori** rispetto a quelle necessarie rispetto alle finalità del trattamento
- Utilizzo delle informazioni sulla localizzazione **per finalità di controllo a distanza dell'attività lavorativa** (es. a fini disciplinari)
- **Interazione con altri sistemi aziendali,** per esempio quelli volti a valutare il corretto adempimento della prestazione lavorativa
- **Utilizzo di funzionalità per le quali non sia stato opportunamente informato l'utilizzatore**
- **Accesso** ai dati relativi alla localizzazione **da parte di persone non autorizzate**
- **Uso promiscuo dei dispositivi** mobili aziendali sia per finalità personali che per finalità lavorative

Le indicazioni dell'ispettorato nazionale del lavoro (circ. N. 2/2016)

- L'art. 4, comma 2, della L. n. 300/1970 stabilisce che **le procedure autorizzatorie indicate dalla disposizione non si applicano "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze**".

- Ciò posto, è pertanto necessario individuare quando l'installazione di apparecchiature di localizzazione satellitare GPS sia strettamente funzionale a "...rendere la prestazione lavorativa...", tenuto conto che l'interpretazione letterale del disposto normativo porta a considerare quali strumenti di lavoro quegli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità sia stati posti in uso e messi a sua disposizione.

- In linea di massima, e in termini generali, si può ritenere che i sistemi di sistemi di geolocalizzazione rappresentino un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro

Le indicazioni dell'ispettorato nazionale del lavoro (circ. N. 2/2016)

- Ne consegue che, in tali casi, la fattispecie rientri nel campo di applicazione di cui al comma 1 dell'art.4 L. n. 300/1970 e pertanto le relative apparecchiature **possono essere installate solo previo accordo stipulato con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione da parte dell'Ispettorato nazionale del lavoro** (art. 4, comma 1, della L. n. 300/1970 come modificato dall'art. 5, comma 2, D.Lgs. n. 185/2016).

- Si evidenzia tuttavia, che solo in casi del tutto particolari - qualora i sistemi di loçalizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa (e cioe la stessa non possa essere resa senza ricorrere all'uso di tali strumenti), ovvero l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00, ecc.) – si può ritenere che gli stessi finiscano per "trasformarsi" in veri e propri strumenti di lavoro e pertanto si possa prescindere, ai sensi di cui al comma 2 dell'art. 4 della L. n. 300/1970, sia dall'intervento della contrattazione collettiva che dal procedimento amministrativo di carattere autorizzativo previsti dalla legge

Privacy e lavoratori

Il garante privacy, ancora nel 2011, ha emanato un PROVVEDIMENTO GENERALE con il quale ha disciplinato la tematica dei sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro.

Fonte: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1850581

Privacy e lavoratori

Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro» - 4 ottobre 2011

Misure prescritte dal Garante

la posizione del veicolo di regola **non deve essere monitorata continuativamente** dal titolare del trattamento, ma **solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite**;

i tempi di conservazione delle diverse tipologie di dati personali eventualmente trattati **devono essere commisurati tenendo conto di ciascuna delle finalità in concreto perseguite**;

Privacy e lavoratori

Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro» - 4 ottobre 2011

Misure prescritte dal Garante

la designazione quali **responsabili del trattamento** degli operatori economici che forniscono i servizi di localizzazione del veicolo e di trasmissione della posizione del medesimo, impartendo loro le necessarie istruzioni in ordine all'utilizzo legittimo dei dati raccolti per le sole finalità previste dall'accordo che regola la fornitura del servizio di localizzazione, con la determinazione delle tipologie di dati da trattare nonché delle modalità e dei tempi della loro eventuale conservazione;

un modello semplificato di **informativa**, utilizzabile alle condizioni indicate in motivazione, al fine di rendere noto agli interessati il trattamento effettuato mediante il sistema di localizzazione del veicolo.

Controlli a distanza sul lavoratore

Le principali norme applicabili al controllo sui lavoratori:

- **L'articolo 6 dello Statuto dei Lavoratori**
  - *Le visite personali di controllo sul lavoratore sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti*

Controlli a distanza sul lavoratore

Le principali norme applicabili al controllo sui lavoratori:

- **L'articolo 7 dello Statuto dei Lavoratori**
  - *Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano*

- **L'articolo 8 dello Statuto dei Lavoratori**
  - *"E' fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore"*

Alcuni riferimenti normativi

- Regolamento UE 2016/679 – GDPR – "General Data Protection Regulation"
- Legge n. 300/1970 - "Statuto dei lavoratori"
- Provvedimento generale del Garante per la protezione dei dati personali del 4 ottobre 2011 "Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro"
- Provvedimento del Garante per la protezione dei dati personali "Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone" (Verifica preliminare richiesta da Ericsson Telecomunicazioni S.p.A. – 11 settembre 2014)
- Provvedimento del Garante per la protezione dei dati personali "Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone" (Verifica preliminare richiesta da Wind Telecomunicazioni S.p.A. – 9 ottobre 2014)
- WP29 – WP251 rev01

Impatti GDPR sul controllo a distanza

Principi del trattamento

liceità, correttezza e trasparenza

limitazione della finalità

minimizzazione dei dati

esattezza

limitazione della conservazione

integrità e riservatezza

Il titolare del trattamento è responsabile del rispetto del principi sopra indicati e deve essere in grado di dimostrarlo («***accountability***») - **Art. 5.2 GDPR**

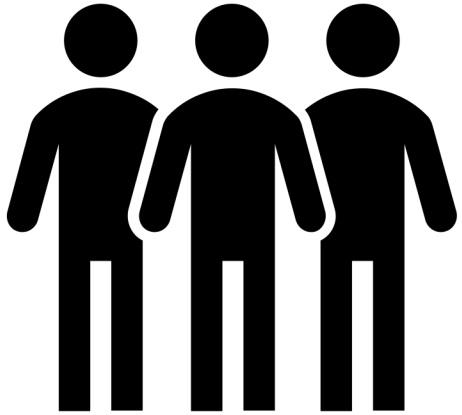
Ruoli Privacy

TITOLARE («*CONTROLLER*»)

«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»

INCARICATI («*PERSONS IN CHARGE OF THE PROCESSING*")

«le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile».



RESPONSABILE («*PROCESSOR*»)

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

INTERESSATO («*DATA SUBJECT*»)

«la persona fisica cui si riferiscono i dati personali».

Obblighi del Responsabile

OBBLIGHI DEL RESPONSABILE:

a) trattare i dati solo su istruzioni documentate del Titolare

b) assicurare che gli incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza

c) adottare tutte le misure tecniche e organizzative ritenute adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 sulla base degli elementi indicati in cima

e) assistere il Titolare con adeguate misure per «dar seguito alle richieste per l'esercizio dei diritti dell'interessato»;

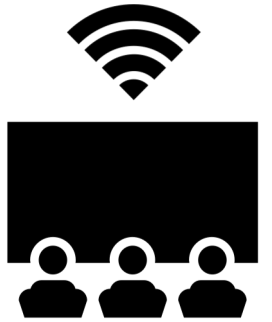
f) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile (il quale, in talune circostanze, è l'unico soggetto in grado di rilevare un *data breach*)

g) cancellare tutti i dati personali o restituire le copie esistenti alla cessazione delle funzioni di Responsabile

h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e collaborazione alle attività di revisione, comprese le ispezioni del Titolare (o soggetto da questi incaricato)

Le novità introdotte dal GDPR:
un approfondimento sulla Data Protection by design

L’innovazione ed il GDPR



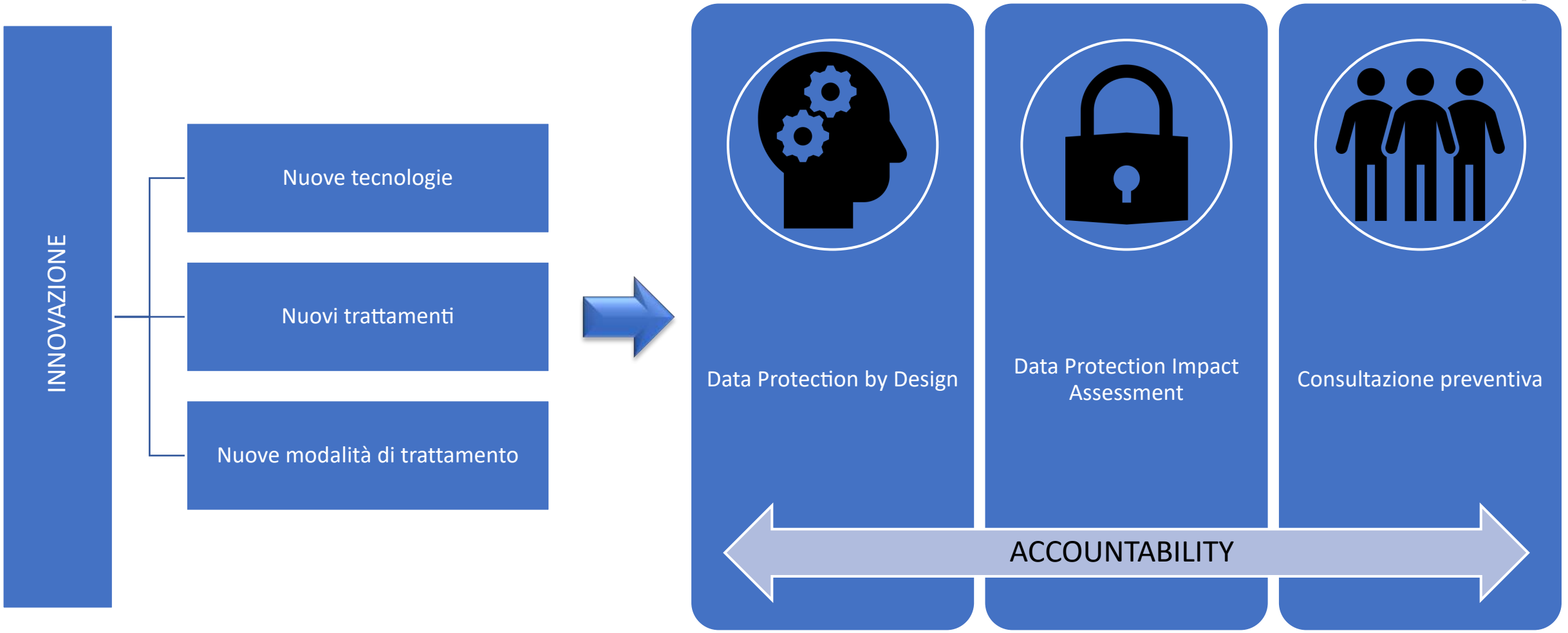
INNOVAZIONE

NUOVE TECNOLOGIE

NUOVI TRATTAMENTI

NUOVE MODALITÀ DI TRATTAMENTO

L'innovazione ed il GDPR



L'innovazione e la privacy by design

Protezione sin dalla progettazione

- **PRIVACY BY DESIGN**
- **SECURITY BY DESIGN**

Le **misure a protezione di dati devono essere adottate già al momento della progettazione di un prodotto o software.**

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire in ogni caso che siano trattati solo i dati necessari per ogni specifica finalità.

Data protection by design

Articolo 25
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto **dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace **i principi di protezione dei dati**, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

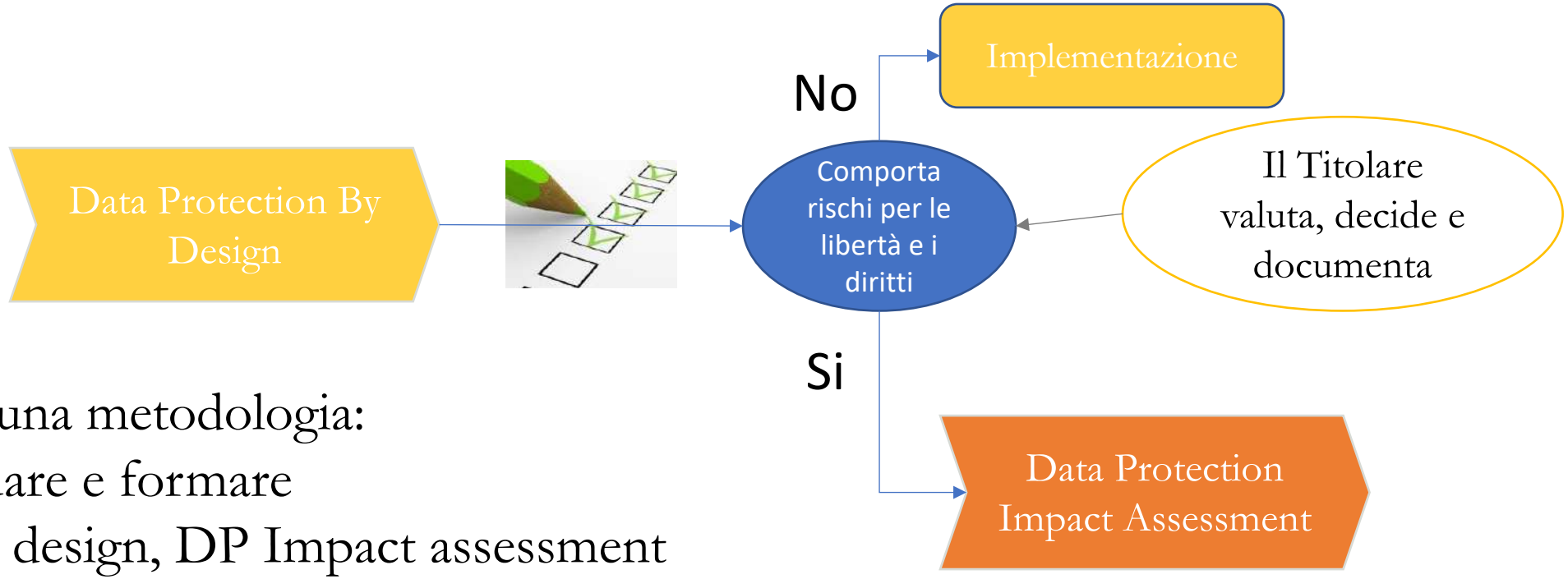
E' pensata per essere una prassi operativa aziendale che riguarda tutti i nuovi trattamenti o la revisione sostanziale di trattamenti in corso.

Riguarda la fisiologia del trattamento, cioè come viene effettuato nella normalità operativa.

Non riguarda solo la sicurezza ma tutti i requisiti che un trattamento deve rispettare.

Richiede una metodologia documentata, non necessariamente complessa

Data protection by design



Una procedura e una metodologia:

- Chi: individuare e formare
- Cosa: DP by design, DP Impact assessment
- Come: metodologia aziendale, linee guida, …
- Quando: change, innovation, update
- Dove: tutti i dipartimenti

Le novità introdotte dal GDPR:
un approfondimento sulla Data Protection Impact Assessment

La data protection impact assessment

Nel valutare se determinate operazioni di trattamento presentino **«rischi elevati per i diritti e le libertà delle persone fisiche»**, potrebbe essere preso in considerazione ad esempio **l'utilizzo di tecnologie o soluzioni organizzative di carattere innovativo**.

In tale ipotesi, il GDPR evidenzia la necessità di porre in essere **una valutazione di impatto**: potrebbe essere sconosciuto l'impatto che l'utilizzo di tale tecnologia ha sui singoli interessati.

L'effettuazione di una DPIA potrebbe dunque aiutare il titolare del trattamento a comprendere i rischi esistenti e a prendere le misure opportune.

La data protection impact assessment

Articolo 35 Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, **allorché prevede in particolare l'uso di nuove tecnologie,** … può presentare **un rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento **effettua, prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla **protezione dei dati personali**.

[…]

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
   a) **una valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, **basata su un trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici …;
   b) **il trattamento, su larga scala**, di categorie particolari di dati personali …; o
   c) **la sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

[...]

La DPIA è richiesta solo per trattamenti innovativi che possono comportare rischi particolari, diversamente dalla DP by design che è una procedura sempre richiesta

La sicurezza è uno dei temi da considerare insieme agli altri diritti dell'interessato

Il Garante può definire un elenco dei trattamenti per cui è obbligatoria ed uno per cui non è richiesta.

DPIA e consultazione preventiva

Articolo 36 Consultazione preventiva

1. Il titolare del trattamento, prima di procedere al trattamento, **consulta l'autorità di controllo qualora la valutazione d'impatto** sulla protezione dei dati […] indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
2. Se ritiene che il trattamento previsto di cui al paragrafo **1 violi il presente regolamento**, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, […], un parere scritto al titolare del trattamento […]
3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:
   a) ove applicabile, le rispettive responsabilità del titolare del trattamento, […] e **dei responsabili del trattamento**…;
   b) le finalità e i mezzi del trattamento previsto;
   c) le misure e le garanzie previste per proteggere i diritti […];
   d) […]

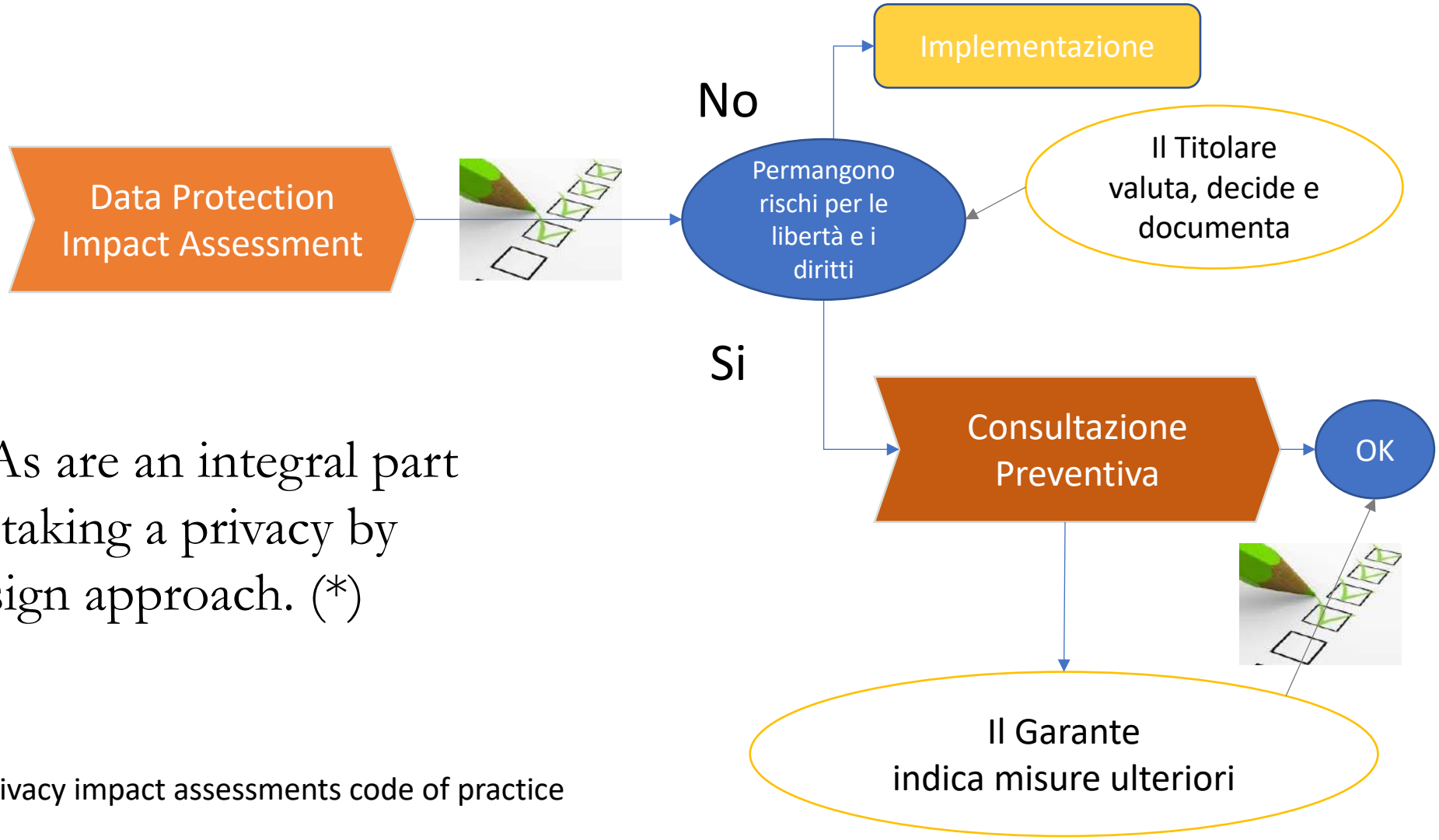
L'esito della valutazione di impatto é decisivo per determinare la necessità di consultazione preventiva del Garante.

Devono quindi essere previste procedure specifiche per assicurare che l'esito della DPIA sia valutato appropriatamente

Il Garante ha un tempo definito (prorogabile) per rispondere

Il Garante può intervenire ex-post

La DPIA



PIAs are an integral part of taking a privacy by design approach. (*)

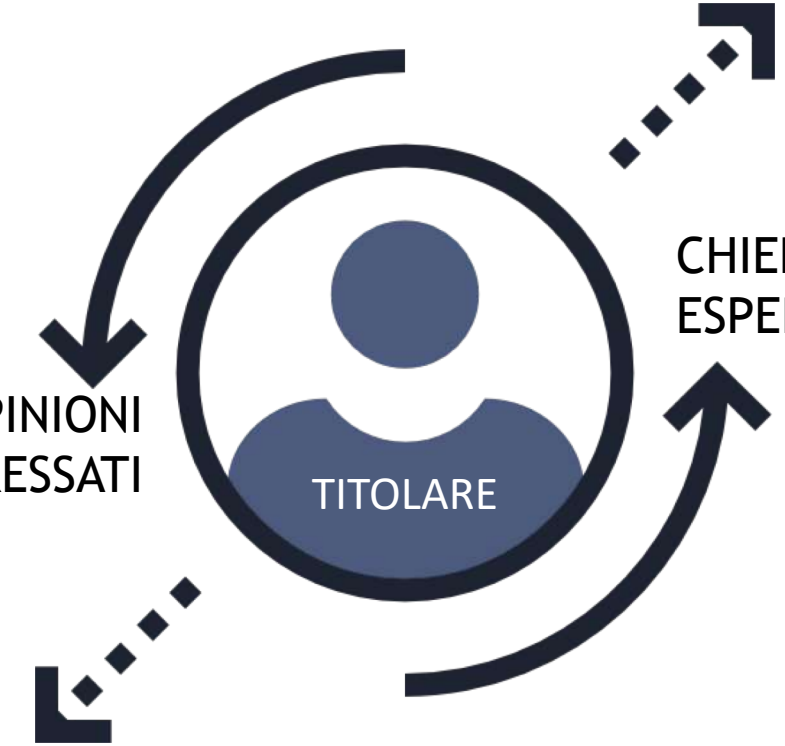
(*) Conducting privacy impact assessments code of practice

Data protection impact assessment

- **Obbligatoria solo per rischi elevati**
- Descrive il trattamento
- Permette di valutare la necessità e la proporzionalità di un trattamento
- Contribuisce a gestire i rischi
- È un processo per la costruzione e la dimostrazione della conformità

Focus DPIA: soggetti coinvolti

DEVE RACCOGLIERE L'OPINIONE DEL DPO



CHIEDE CONSULENZA AD ESPERTI INDIPENDENTI
se del caso

DEVE RACCOGLIERE LE OPINIONI DEGLI INTERESSATI
se del caso

È OBBLIGATO A VERIFICARE CHE LA DPIA VENGA ESEGUITA

La Geolocalizzazione nel rapporto di lavoro: Il Data Protection Working Party Article 29

WP249

- Il *Data Protection Working Party Article 29* ha emanato, in **data 8 Giugno 2017**, l'Opinion *2/2017 r*elativa al Trattamento dei dati in contesto lavorativo.

- Si tratta dell'evoluzione dei precedenti pareri in materia (il WP48 del 2001 e il WP55 del 2002) promossi dallo stesso organo alla luce del nuovo GDPR.

- Nuova valutazione **dell'equilibrio tra il legittimo interesse dell'azienda e le ragionevoli istanze di tutela della privacy del lavoratore** alla luce dei nuovi rischi legati ai nuovi scenari introdotti dallo sviluppo tecnologico.

WP249

Guardando nella direzione del GDPR, quando si trattano dati personali di lavoratori:

- Le aziende dovrebbero tenere sempre presente i principi fondamentali della protezione dei dati, **indipendentemente dalla tecnologia utilizzata**;

- I **contenuti delle comunicazioni elettroniche** inoltrate dai locali aziendali devono ricevere stessi diritti fondamentali di protezione propri delle altre tipologie di comunicazioni;

- **Il consenso al trattamento dei dati in contesto lavorativo è difficilmente raccordabile ad una base legale**, in quanto spesso viziato dal fatto che i lavoratori non possono rifiutarsi senza il timore di subire possibili conseguenze;

WP249

Guardando nella direzione del GDPR quando si trattano dati personali di lavoratori:

- **L'esistenza di un contratto o di un legittimo interesse al trattamento** possono essere presi in considerazione **solo quando il trattamento è strettamente necessario al raggiungimento di una finalità legittima e nel rispetto del principi di proporzionalità e sussidiarietà**;

- I lavoratori dovrebbe **ricevere chiare informazioni sulle attività di monitoraggio attivate dall'organizzazione**;

Rischi

Oltre i RISCHI esaminati in precedenza, con riferimento al tema della geolocalizzazione, si deve considerare che:

- l'utilizzo massivo di tecnologie di monitoraggio potrebbe far venir meno l'inclinazione del lavoratore ad informare l'azienda su irregolarità o illeciti commessi da parte dei superiori e/o colleghi a danno dei beni aziendali e del business in generale (whistleblowing).

- In questi casi, infatti, l'anonimità è sinonimo di garanzia.

Rischi

In relazione agli scenari di rischio relativi al trattamento dei dati personali dei lavoratori attraverso l'utilizzo di nuove tecnologie, ogni datore di lavoro dovrebbe considerare se tale trattamento:

- è strettamente necessario in relazione alla base giuridica per la quale esso è svolto;
- è effettuato in maniera corretta nei confronti dei lavoratori;
- è proporzionato alla finalità che persegue;
- è reso sufficientemente chiaro e trasparente nelle sue modalità di attuazione.

Durante il processo di reclutamento

- L'azienda, prima di accedere ai *social media profile* del candidato, dovrebbe verificare se quest'ultimo sia relativo alla sfera privata della persona.
- Questo potrebbe essere un indicatore significativo della liceità del trattamento.
- Il datore di lavoro non è giustificato dal compiere investigazioni e/o trattamenti sulle informazioni presenti sui profili social network del candidato lavoratore anche se quest'ultimo ha impostato la privacy del profilo personale in modalità 'open'.

Durante il processo di reclutamento

Il trattamento dei dati richiede un preesistente fondamento giuridico basato sul legittimo interesse alla raccolta, che deve risultare necessaria e rilevante in relazione alla job position per la quale ci si è candidati.

L'interessato deve comunque esserne informato preventivamente e i dati raccolti devono essere cancellati non appena perdono rilevanza.

In nessun caso si può richiedere al candidato di 'stringere amicizia' o comportamenti similari per carpire informazioni personali.

Esempio:

Una azienda in fase di selezione, in base all'articolo 7(f) del DPD, può eseguire un controllo sui profili personali dei candidati su vari social network (sulle informazioni disponibili al pubblico) e includere le informazioni raccolte nel processo di screening solamente se:

- è strettamente correlato ad esigenze lavorative (es. la capacità di valutare i rischi specifici connessi ai candidati per specifiche funzioni);

- I candidati ne sono correttamente informati (es. nel testo del job alert).

In-employment screening

Le aziende devono astenersi dall'effettuare monitoraggi, soprattutto se permanenti e su larga scala, sulle attività dei lavoratori sui propri *social media profile* personali, acquisendo così informazioni personali e sensibili su amici, familiari, opinioni, credenze, interessi, abitudini, luoghi, attitudini, comportamenti fino alla loro condivisione di informazioni con terzi.

Devono, altresì, evitare dal far utilizzare al lavoratore il proprio *social network profile* personale per scori professionali ('portavoce', ecc.) specificandolo chiaramente nelle *terms and conditions* del contratto di lavoro.

Esempio:

- Un azienda monitora i profili LinkedIn di ex-lavoratori che abbiamo sottoscritto clausole contrattuali di non concorrenza allo scopo di verificare il rispetto delle stesse da parte di quest'ultimi per tutta la durata del divieto.
- Se il titolare riesce a provare che non esistono sistemi meno invasivi e che i lavoratori sono stati adeguatamente informati a riguardo, ci si può basare sul legittimo interesse ex art. 7(f) del DPD.
- Il monitoraggio deve, però, limitarsi solamente a questa tipologia di lavoratori.

Uso di soluzioni ICT sul luogo di lavoro

Lo sviluppo tecnologico ha reso disponibili nuovi strumenti di monitoraggio sull'attività dei lavoratori molto invasivi tra cui:

- Strumenti di *Data Loss Prevention (DLP);*
- *Next-Generation Firewalls* (NGFWs) e *Unified Threat Management* (UTM);
- *Applicazioni di sicurezza e misure che comportano l'accesso 'loggato' del lavoratore ai sistemi aziendali*;
- *eDiscovery technology*, a scopo probatorio;
- tracking delle applicazioni e device con software invisibili su desktop e/o cloud;
- Applicazioni cloud service a controllo dei logging del lavoratore;
- Monitoraggio dei device (e.g., PCs, mobile phones, tablets), in uso ai lavoratori per policy interne (vd. *Bring-Your-Own-Device* –BYOD- o *Mobile Device Management* –MDM-); e
- L'uso dei device "indossabili" (e.g., health e fitness device).

Esempio:

- Un'azienda vuole implementare un dispositivo per le ispezioni sul traffico TLS per decifrare il traffico per rilevare attività malevola, registrando e analizzando l'intera attività online svolta dal lavoratore all'interno del network aziendale.

- **Fondamento giuridico:**
  - legittimo interesse di proteggere il network, i dati dei lavoratori e dei clienti ivi conservati contro accessi abusivi e perdite di dati.

Lesione del **principio di proporzionalità** e del **diritto alla segretezza delle comunicazioni connesso al monitoraggio di tutte le attività online del dipendente.**

Il datore di lavoro, quindi, dovrebbe in primo luogo veriuficare se esitano altri mezzi, a garanzia della sicurezza della rete e della confidenzialità dei dati.

Uso di soluzioni ICT sul luogo di lavoro

In alternativa:

- evitare il monitoraggio permanente dei log generati dall'attività del lavoratore,
- prevedere alert in grado di segnalare il verificarsi di incident,
- un accesso alternativo libero da monitoraggi (attraverso il free Wi-Fi o stand-alone device o terminali aziendali ad uso privato).
- minimizzare la raccolta di informazioni.

Occorre prevedere una **policy**:

- che specifichi i casi e da chi e come (es. con quali strumenti) i log possano possono essere resi accessibili
- che sia accessibile a tutti
- che contenga i permessi e i divieti sull'uso del network e delle facilities.
- che venga revisionata almeno annualmente, per valutare i monitoraggi adottati e verificare la disponibilità di eventuali tool alternativi meno invasivi.

Indipendentemente dalle tecnologie adottate e dalle caratteristiche possedute, la base legale per il trattamento dei dati prevista all'articolo 7(f) del DPD prevede le seguenti condizioni:

- Il rispetto del principio di proporzionalità delle misure adottate;
- L'adozione di azioni aggiuntive per mitigare l'impatto del trattamento (e.g. prevedere un DPIA preventiva);
- L'adozione di policy (che in alcuni paesi deve ricevere l'approvazione delle rappresentanze sindacali);

Esempio
(data loss prevention)

Un azienda adotta un tool di *Data Loss Prevention* che monitori automaticamente tutte le mail in uscita a protezione dei dati personali dei clienti e dei dati relativi ai suoi asset per prevenirne l'accesso e la trasmissione non autorizzata.

Occorre rispettare sia il legittimo interesse dell'azienda sia il diritto fondamentale di protezione dei dati personali.

COME?

Le regole che il sistema segue per caratterizzare una singola mail come fonte di data breach dovrebbero essere accessibili *in toto* all'utilizzatore.

In caso venga segnalata una mail in particolare, il tool dovrebbe emettere un messaggio di *warning* che informi l'autore prima dell'invio, per consentirgli di cancellare la trasmissione

In molti casi, il monitoraggio dei lavoratori è possibile non attraverso l'utilizzo di specifiche tecnologie, ma semplicemente per il fatto che ai dipendenti venga richiesto di utilizzare applicazioni fornite dal datore di lavoro che trattano dati personali. Si consideri ad esempio l'utilizzo di applicazioni cloud per la generazione di documenti, calendari o di social networking.

Dovrebbe essere assicurato ai lavoratori l'utilizzo di determinati spazi ad uso privato ai quali l'azienda non può avere accesso se non in circostanze eccezionali. (soprattutto per i calendar spesso usati per programmare attività della sfera privata).

Ad esempio, a volte, il rispetto del principio di sussidiarietà significa poter evitare qualsiasi attività di monitoraggio. Ad esempio è possibile bloccare l'accesso ai siti web piuttossto che monitorare continuamente tutte le comunicazioni.

Soluzioni ICT al di fuori del luogo di lavoro

Con le nuove forme dell'homeworking, del remote working e delle relative *"bring your own device" policies*, l'uso di soluzioni ICT fuori del luogo di lavoro è diventato molto comune.

Questo pone a rischio la vita privata del lavoratore poiché spesso i sistemi di monitoraggio si estendono –di fatto- anche ai luoghi domestici e privati qualora il lavoratore si trovi ad utilizzare tali strumenti.

Monitoraggio a casa o in remote working

Spesso le aziende offrono ai lavoratori la possibilità di lavorare in remoto dotando quest'ultimi di strumenti ICT o software i quali permettono di avere ovunque le risorse proprie del luogo di lavoro.

Il *remote working*, pur avendo aspetti di sviluppo certamente positivi, presenta diversi e nuovi profili di rischio per le aziende:

- non sottostà alle regole in materia di sicurezza sui luoghi di lavoro;
- senza l'implementazione di adeguate misure di sicurezza aumenta il rischio di accesso non autorizzato fino alla perdita o distruzione di informazioni, incluse i dati personali di lavoratori o clienti.

Monitoraggio a casa o in remote working

Le aziende potrebbero essere portate a ritenere giustificabile l'implementazione di soluzioni software in grado di rilevare:

- i movimenti di tasti e mouse,
- lo screen capturing (a random o a intervalli),
- il logging dell'uso delle applicazioni (e per quanto tempo)
- raccogliere immagini via webcam.

In questi casi, difficilmente l'azienda può agire legittimamente sulla base di un legittimo interesse.

Occorrerà, dunque, ridurre il rischio rispettando i principi di proporzionalità e non eccessività a prescindere dalla soluzione adottata.

Device personale per scopi di lavoro (BYOD)

Talvolta i lavoratori usano il proprio device personale per usi lavorativi.
Il fenomeno prende il nome di "bring your own device" (BYOD).

I rischi privacy, in questo caso, sono associati ai security scan che permettono l'accesso a tutti i dati contenuti nel device.

Le aziende, quindi, potenzialmente potrebbero trovarsi a trattare informazioni personali del lavoratore e dei suoi familiari.

Occorre implementare misure appropriate che distinguano tra uso privato e lavorativo del device.

Le aziende si possono dotare di soluzioni in grado di trasferire in modo sicuro i dati tra il device e il network aziendale, dirigendone il traffico attraverso un VPN nel network aziendale.

A tutela dell privacy del lavoratore, esistono diverse soluzioni:

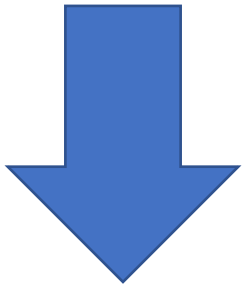
- Device con protezioni aggiuntive -come la "sandboxing" data- che mantengono i dati all'interno di una specifica app.

- l'azienda può proibire l'uso privato di alcuni tipi di device aziendali qualora non ci sia modo di evitare il monitoraggio dell'uso privato dello stesso.

La trasferibilità transfrontaliera dei dati

Le aziende spesso utilizzano soluzioni cloud-based per gestire HR-data online.

Questo si traduce, a volte, in un trasferimento internazionale extra-UE di dati relativi ai lavoratori, che il GDPR permette solamente laddove si garantiscono adeguati livelli di protezione.



Occorre assicurare che la condivisione dei dati extra EU/EEA ed il loro accesso da parte di terze parti rimanga limitato al minimo necessario all'interno della finalità che si intende perseguire.

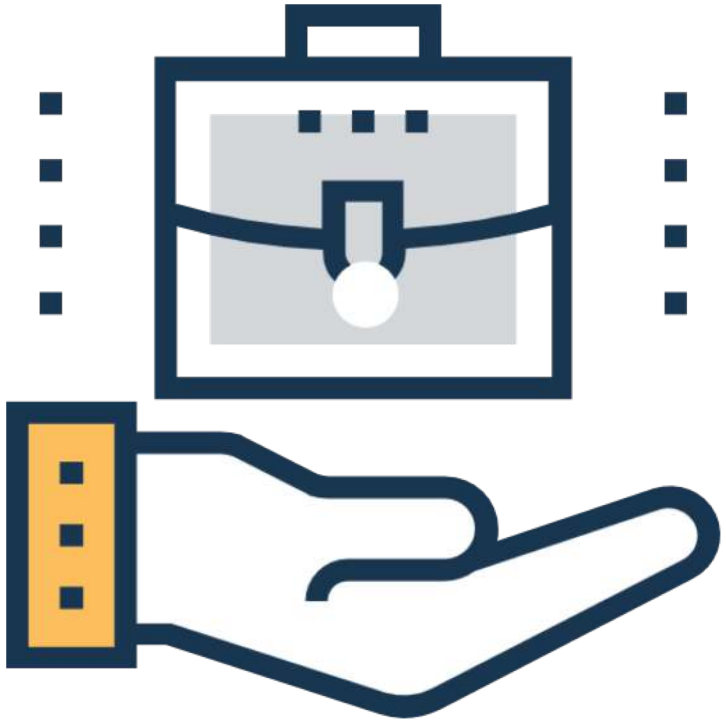
La Geolocalizzazione nel rapporto di lavoro: Il legittimo interesse

Il legittimo interesse

Non essendo possibile ravvisare nel CONSENSO una valida base giuridica, è NECESSARIO valutare invece la possibilità di utilizzare altri basi giuridiche disciplinate dal GDPR ed in particolare il:

LEGITTIMO INTERESSE

Il Legittimo interesse (art. 6 co. 1, lett. F)



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

Il titolare deve effettuare un **BILANCIAMENTO** fra l'interesse legittimo proprio/di terzi e i diritti dell'interessato.

Il legittimo interesse – Bilanciamento di interessi

Affinché il Titolare possa basare il trattamento su tale condizione di liceità è necessario che **NON prevalgano** gli **interessi** o i diritti e le libertà fondamentali dell'interessato.

Interesse legittimo del titolare

Interessi e diritti dell'interessato

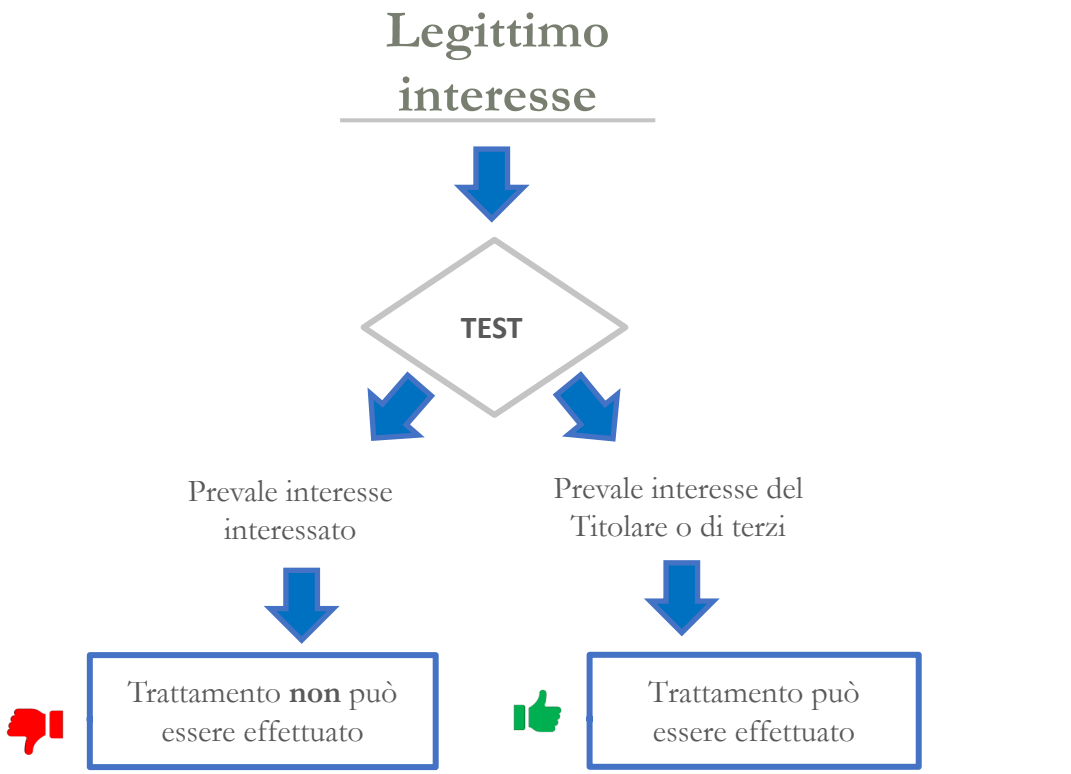
Il risultato del test di bilanciamento determinerà se il titolare **può fondare o meno il trattamento su tale base giuridica.**

Il legittimo interesse – Il test di bilanciamento

Altre basi giuridiche:

- **Consenso**
- **Esecuzione contratto**
- **Obbligo legale**
- **Salvaguardia interessi vitali**
- **Compito interesse pubblico**

Il trattamento è lecito *a priori* (si considera quindi soddisfatto il bilanciamento tra interessi del titolare/terzi e dell'interessato) ed è subordinato solo all'osservanza delle altre disposizioni normative applicabili.



Il test deve basarsi su elementi oggettivi, in quanto la valutazione di legittimità potrebbe essere sempre smentita da parte dell'Autorità, in tutti i casi in cui il legittimo interesse non corrisponda ad uno degli esempi cristallizzati in via generale nella norma o in provvedimenti del Garante.

Il legittimo interesse - le ragionevoli aspettative dell'interessato

Oltre al presente bilanciamento, occorrerà considerare, così come ulteriormente indicato nel considerando 47 del GDPR, anche "*le ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento*".

Lista non esaustiva di fattori chiave

Il WP29, nell'Opinion 6/2014 precisa che il bilanciamento consiste nel confrontare tra loro due "pesi" facilmente quantificabili e comparabili. Per eseguire il test occorre invece valutare appieno una serie di fattori in modo da garantire che gli interessi e i diritti fondamentali degli interessati siano tenuti nella debita considerazione. Al tempo stesso, il test comparativo è adattabile, può variare da semplice a complesso e non deve risultare indebitamente gravoso.

I fattori di cui tenere conto nell'esecuzione del test di bilanciamento includono:

- la natura dell'interesse legittimo, se il trattamento è necessario per l'esercizio di un diritto fondamentale o effettuato nell'interesse pubblico o sia riconosciuto dalla collettività interessata, considerando il possibile pregiudizio che deriverebbe per il Titolare qualora non effettuasse il trattamento;
- gli impatti sugli interessati e le loro ragionevoli aspettative su ciò che accadrà ai loro dati, nonché la natura dei dati e le modalità di trattamento;
- la presenza di garanzie supplementari che potrebbero limitare gli impatti del trattamento sugli interessati, quali la minimizzazione dei dati, le tecnologie di rafforzamento della tutela della vita privata, una maggiore trasparenza, il diritto generale e incondizionato di "opt-out" e la portabilità dei dati.

Il legittimo interesse (art. 6 co. 1, lett. F)

BILANCIAMENTO DI INTERESSI

I titolari dovrebbero condurre la propria valutazione alla luce dei requisiti indicati dal Garante nei propri provvedimenti in materia di bilanciamento di interessi, con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorità, nonché facendo riferimento al documento pubblicato dal WP29 sul punto (WP217).

Affinché l'interesse sia «legittimo» deve essere:

- **lecito** (cioè perseguito in accordo con i principi di protezione dei dati e, più in generale, non *contra legem);*
- **sufficientemente articolato** per consentire il bilanciamento d'interessi;
- **reale** ed **attuale**, cioè deve corrispondere ad un beneficio atteso in un prossimo futuro.

Il legittimo interesse (art. 6 co. 1, lett. F)

Distinzione fra «interesse» e «finalità»

L'interesse legittimo è il generico beneficio che il titolare ottiene dal trattamento, la finalità invece è la ragione ultima per la quale i dati vengono trattati, rappresenta cioè l'obiettivo oggettivo del trattamento.

Come precisato dal WP29 nell'Opinion 6/2014 una società che fornisce **energia nucleare** può avere un interesse nell'assicurare la salute e la sicurezza dei suoi dipendenti. Per tale ragione, la società adotta delle procedure di controllo dell'accesso ai propri impianti mediante il trattamento di alcuni dati dei propri dipendenti.

Pertanto

la «**finalità**» del trattamento è il controllo dell'accesso ai propri impianti

l'«**interesse**» perseguito è quello di garantire la sicurezza dei propri dipendenti

Il legittimo interesse (art. 6 co. 1, lett. F)

La comunicazione al Garante

Con la Legge di bilancio 2018 (legge n. 205 del 27 dicembre 2017) era stato introdotto, all'art. 1, comma 1022, **una particolare procedura di (previa) comunicazione al Garante**, allorquando il Titolare del trattamento, usando *nuove tecnologie* o *strumenti automatizzati* avesse deciso di applicare la presente base giuridica.In particolare, veniva stabilito l'obbligo di compilare e inviare al Garante un'informativa contenente *l'oggetto*, le *finalità* ed il *contesto* del trattamento. Trascorsi, poi, 15 giorni lavorativi dall'invio della presente informativa, in assenza di risposta da parte dell'Autorità o salvo eventuale istruttoria (ove l'Autorità avesse ravvisato il rischio che di una lesione dei diritti e delle libertà dei soggetti interessati), si sarebbe, dunque, potuto procedere al trattamento.

Questo comma **è stato emendato dal D.lgs 101/2018**. All'art. 22, n.5, è stato precisato che il su richiamato comma 1022 si applica: «… *esclusivamente ai trattamenti dei dati personali funzionali all'autorizzazione del cambiamento del nome o del cognome dei minorenni*».

La Geolocalizzazione nel rapporto di lavoro: Privacy e Statuto dei Lavoratori

La Geolocalizzazione nel rapporto di lavoro: Casi Pratici

Il caso Manpower - 2016

- Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze.

- installazione di una specifica **applicazione** - contenente una funzionalità di localizzazione geografica - sul dispositivo smartphone dei dipendenti, preordinata all´effettuazione della "timbratura del cartellino e la rilevazione delle presenze" (cfr. istanza 18.12.2015, p. 1).
- Tale applicazione, sviluppata da Peoplelink s.r.l., è configurata in modo tale da consentire l´accesso - previa autenticazione con user id e password - al dipendente, che "cliccherà su icona "ingresso" per indicare l´inizio dell´attività lavorativa e su "uscita" per indicare la fine della giornata lavorativa" (cfr. istanza cit., p. 1 e 2).
- *«Il trattamento dei dati personali dei dipendenti sottoposto a verifica preliminare consente di rilevare la localizzazione geografica di dispositivi smartphone di proprietà dei lavoratori (e, indirettamente, la posizione geografica dei lavoratori medesimi) attraverso l´attivazione di una applicazione finalizzata alla rilevazione della presenza in servizio.*

- ***«il trattamento presenta rischi specifici per la libertà, i diritti e la dignità del dipendente»***

Fonte: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5497522

Il caso Manpower - 2016

- *«[…] il sistema prospettato consente, rispetto a tali rapporti di lavoro (quantificati dalle società nell´ordine di decine di migliaia stipulati ogni anno), di realizzare* ***significativi risparmi di gestione*** *(con l´eliminazione dei lettori di badge, quando collocati presso gli utilizzatori) nonché di semplificare ed incrementare l´efficienza e la certezza dell´attività di rilevazione delle presenze dei lavoratori somministrati, anche in vista di possibili abusi. Ciò risulta anche favorire l´effettiva certificazione delle ore lavorate nonché, più radicalmente, dell´avvenuta effettuazione della prestazione lavorativa in somministrazione a favore dell´utilizzatore, a tutela dei diritti riconosciuti dall´ordinamento in primo luogo al lavoratore e anche alle parti del contratto di somministrazione […]»*

- *«[…] alla luce delle valutazioni sopra esposte circa la conformità del sistema ai principi di protezione dei dati e considerate le misure poste a tutela degli interessati indicate nel successivo paragrafo 7, che i descritti trattamenti possano essere effettuati, nei confronti dei dipendenti, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. "bilanciamento di interessi", individua un legittimo interesse al trattamento di tale tipologia di dati in relazione alle finalità rappresentate (art. 24, comma 1, lett. g), del Codice).»*

Il caso Manpower - 2016

Il Garante, preso atto della presente richiesta di verifica preliminare:

- stabilisce che il trattamento dei dati personali dei dipendenti, possa essere effettuato mediante il descritto applicativo nei termini di cui in motivazione;

- prescrive che le società, quali misure necessarie, dovranno, nell´utilizzo del sistema:
  - **cancellare** il dato relativo alla posizione del lavoratore, avendo verificato preventivamente l´associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore, conservando, eventualmente, il solo dato relativo alla predetta sede di lavoro, alla data e all´orario cui si riferisce la timbratura;
  - **configurare il sistema** in modo tale che sul dispositivo sia posizionata un´icona che indichi che la funzionalità di localizzazione è attiva;
  - **adottare specifiche misure** idonee a garantire che l´applicativo installato sul dispositivo del dipendente non possa effettuare trattamenti di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o alla navigazione in internet o altro);

- rammenta la necessità di […] di fornire ai dipendenti un´informativa completa di tutti gli elementi previsti […], di effettuare la designazione di incaricati e responsabili, di adottare le misure di sicurezza previste […], di predisporre misure al fine di garantire agli interessati l´esercizio dei diritti previsti […].

Il caso Sicuritalia S.P.A. - Verifica preliminare – 18 aprile 2018

RICHIESTA

Trattamento dei dati personali connesso alla prospettata installazione di una applicazione, completa di funzionalità di localizzazione geografica, **sui dispositivi smartphone o tablet consegnati alle guardie particolari giurate incaricate di effettuare i servizi di vigilanza forniti dalla società**.

COME

L'applicazione verrà attivata dalla guardia mediante l'inserimento del proprio codice identificativo nonché di una password fornita dalla centrale operativa in relazione allo specifico servizio assegnato, immediatamente prima l'inizio del turno.

TUTELA DEGLI INTERESSATI

Considerata la particolarità dei dati trattati, il sistema dovrà essere configurato in modo tale che sul dispositivo aziendale sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva.
Deve inoltre essere prevista la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa, informando correttamente i dipendenti sui casi in cui è consentito disattivare la localizzazione nonché sulle conseguenze degli eventuali abusi.

Il caso Sicuritalia S.P.A. - Verifica preliminare – 18 aprile 2018

PRIVACY

Le finalità del sistema consisterebbero nella necessità di assicurare: "la sicurezza della pattuglia"; la "razionale assegnazione e distribuzione degli interventi alle pattuglie di zona"; il "corretto svolgimento dell'ordinaria attività di vigilanza/ispezione".
I dati raccolti saranno conservati per un periodo non superiore alle ore 24, fatte salve speciali esigenze di ulteriore conservazione.

CARATTERISTICHE

a) l'applicazione prevede un comando di invio «aggressione - panico»; decorsi 30 secondi dall'attivazione del comando **è possibile inviare un allarme immediato** oppure impostare un allarme ritardato e annullabile, allo scadere del quale viene inviata una segnalazione in Centrale Operativa;

b) il sistema consente alla Centrale Operativa di assegnare un allarme proveniente dal sito di un cliente alla pattuglia svolgente servizio in prossimità dello stesso. Qualora la guardia giurata accetti l'incarico e raggiunga la destinazione, può trasmettere la dichiarazione «arrivato sul posto»;

c) la posizione della pattuglia è rilevata ogni 120 secondi ed è prevista la visualizzazione in tempo reale al fine di garantire il più possibile la sicurezza personale degli addetti in servizio;

d) i dati raccolti dal sistema possono essere consultati dagli addetti alla centrale (debitamente nominati incaricati del trattamento), che saranno muniti di apposite credenziali di autenticazione;

e) è escluso l'utilizzo di tali dati da parte della società istante per finalità di controllo dei dipendenti ovvero per scopi disciplinari

Il caso Sicuritalia S.P.A. - Verifica preliminare – 18 aprile 2018

LICEITÀ DEL TRATTAMENTO

L'adozione di un sistema completo di funzionalità di localizzazione da installare su dispositivi forniti ai dipendenti, al fine di rafforzare la sicurezza di persone e beni, nonché per realizzare miglioramenti nell'efficienza dei servizi, risulta in termini generali lecito.
È conforme a quanto stabilito dall'articolo 4, comma 1, della legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) la prospettata attivazione della procedura di garanzia prevista dalla richiamata disciplina in materia di controlli a distanza.

RISPETTO DEI PRINCIPI

Le modalità di trattamento dei dati personali da parte del sistema tecnologico prospettato prevedono, in particolare, **la pseudonimizzazione dei dati delle guardie giurate, che risultano pertanto non già direttamente identificate dal sistema bensì indirettamente identificabili attraverso il raffronto con le credenziali di accesso all'applicazione e con il file compilato dal capo zona ad inizio turno contenente l'associazione guardia giurata/dispositivo**.
L'accesso in tempo reale ai dati di localizzazione effettuato dal personale autorizzato presente nella centrale operativa **è previsto esclusivamente in caso di necessità ed emergenza, ossia in caso di allarme lanciato dalla medesima guardia giurata oppure in caso di avvenuta ricezione di segnalazione di allarme o in caso si rendese necessario procedere ad ispezioni in loco**, oppure in caso di attivazione della funzionalità "**eccesso sosta",** ossia un meccanismo di allarme automatico che scatta in caso di assenza di movimento per un periodo di tempo predeterminato.

Il caso Sicuritalia S.P.A.

Il Garante, preso atto della presente richiesta di verifica preliminare:

- ammette il trattamento di dati personali da parte di Sicuritalia S.p.A. mediante il sistema di localizzazione geografica dei dispositivi aziendali, illustrato nei termini di cui in motivazione, e prescrive che la società, quali misure necessarie, debba:
    - configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva;
    - configurare il sistema in modo da **consentire la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa**;
    - configurare il sistema in modo da **oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività** dell'operatore sul monitor presente nella centrale operativa relativamente a tale funzionalità;
    - individuare profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili;
    - individuare i tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite;
    - predisporre i rapporti per i clienti privi di qualunque riferimento che consenta l'identificazione di dipendenti;
    - procedere alla designazione quale responsabile esterno del trattamento il fornitore del software NavNet;
    - predisporre periodiche verifiche di test sulla funzionalità "eccesso sosta" e l'affidabilità dei parametri adottati, in vista della valutazione di eventuali falsi positivi o negativi effettuati dal sistema e la conseguente predisposizione di correttivi a tutela della qualità dei dati trattati.

• L'IDENTIFICAZIONE BIOMETRICA

Aspetti introduttivi

Il concetto di dato biometrico.
Dal Codice Privacy al Regolamento

L'art. 4 del Codice Privacy, rubricato «Definizioni», riporta la seguente elencazione di dati «sensibili»: «…*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*», senza fornire alcuna indicazione di cosa siano i dati biometrici.

Il GDPR, invece, all'art.4, tra le «Definizioni», contempla una voce specifica sui *dati biometrici*, ovvero quei dati: «…*personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*», che viene poi inserita all'art.9, co.1, nella categoria di dati particolari (ex «dati sensibili» del Codice Privacy).

I sistemi biometrici

Nozione

- I dati biometrici sono dati ricavati dalle **caratteristiche fisiche o comportamentali della persona** a seguito di un apposito procedimento (in parte automatizzato) e poi risultanti in un **modello di riferimento**.

- Quest'ultimo consiste in un insieme di **valori numerici ricavati**, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso **opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.**

I sistemi biometrici

Principi da rispettare

- **Liceità del trattamento**

  - **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 particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad **"aree sensibili",** considerata la natura delle attività ivi svolte: si pensi, ad esempio, **a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore.**

I sistemi biometrici

Principi da rispettare

- **Sistemi di rilevazione biometrica**

  - Nei casi in cui l'uso dei dati biometrici è consentito, la **centralizzazione** in una banca dati delle informazioni personali trattate nell'ambito di un procedimento di riconoscimento biometrico risulta di regola **sproporzionata e non necessaria.**

  - Deve ritenersi adeguato e sufficiente avvalersi di sistemi efficaci di verifica e di identificazione biometrica basati **sulla lettura delle impronte digitali memorizzate, tramite il modello cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (una smart card o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo** (essendo sufficiente attribuire a ciascun dipendente un codice individuale).

I sistemi biometrici

Principi da rispettare

- **Sistemi di rilevazione biometrica**
  - Tale modalità di riconoscimento, infatti, è idonea ad assicurare che possano accedere all'area riservata solo coloro che, autorizzati preventivamente, **decidano su base volontaria di avvalersi della carta o del dispositivo analogo.**
  - Il confronto delle impronte digitali con il modello memorizzato sulla carta o sul dispositivo può essere realizzato ricorrendo **a comuni procedure di confronto sulla carta o dispositivo** stesso, **evitando così la costituzione di un archivio di delicati dati biometrici.**
  - Del resto, in caso di smarrimento della carta o dispositivo, sono allo stato circoscritte le possibilità di **abuso rispetto ai dati biometrici ivi memorizzati**.

I sistemi biometrici

Principi da rispettare

- **Consenso**
  - I dati personali necessari per realizzare il modello possono essere trattati esclusivamente **durante la fase di registrazione**; per il loro utilizzo, il titolare del trattamento deve raccogliere il preventivo **consenso esplicito** degli interessati.

- **Misure di sicurezza**
  - In aggiunta alle misure di sicurezza minime prescritte dal Codice/GDPR, devono essere adottati ulteriori accorgimenti a protezione dei dati, impartendo agli incaricati apposite istruzioni scritte alle quali attenersi, **con particolare riguardo al caso di perdita o sottrazione delle carte o dispositivi loro affidati.**

  - I dati memorizzati devono essere **accessibili al personale preposto al rispetto delle misure di sicurezza all'interno dell'impres**a, per l'esclusiva finalità della verifica della loro osservanza (**rispettando peraltro la disciplina sul controllo a distanza dei lavoratori: art. 4, comma 2, l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice).**

I sistemi biometrici

Principi da rispettare

- **Tempi di conservazione**
  - I dati raccolti non possono essere di regola conservati per un arco di tempo superiore a **sette giorni** e vanno assicurati, anche quando tale arco temporale possa essere lecitamente protratto, idonei meccanismi di cancellazione automatica dei dati.

- ~~**Verifica preliminare**~~

  —

  - ~~Resta salva, per fattispecie particolari o in ragione di situazioni eccezionali non considerate nelle linee guida, la presentazione da parte di Titolari del trattamento che intendano **discostarsi dalle presenti prescrizioni**, di apposito interpello al Garante, ai sensi dell'art. 17 del Codice.~~

I sistemi biometrici

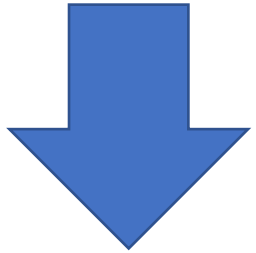
Ulteriori adempimenti necessari

- **Informativa**
  - In base all'art 13 del Codice/GDPR è necessario **informare preventivamente** i dipendenti della finalità della raccolta e del tipo di dati che si intendono trattare.

• LA VIDEOSORVEGLIANZA

Domande ricorrenti:

- E’ possibile installare telecamere all’interno del posto di lavoro?
- Ci sono particolari cautele da adottare?
- E’ possibile registrare le immagini prodotte dalle telecamere?
- Per quanto è possibile conservare le immagini?



Videosorveglianza: Provvedimento generale del Garante dell’8 aprile 2010

La videosorveglianza

Principi da rispettare:

- **Informativa**
  - I cittadini che transitano nelle aree sorvegliate devono essere **informati** della rilevazione dei dati. L'informativa (della quale il Garante ha anche messo a disposizione un modello semplificato: un cartello con un simbolo ad indicare l'area videosorvegliata) deve essere chiaramente visibile ed indicare chi effettua la rilevazione delle immagini e per quali scopi.
  - Il Provvedimento dell'8 aprile 2010 specifica che il cartello deve avere un formato ed un posizionamento tale da risultare chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

La videosorveglianza

Principi da rispettare:

- **Informativa**
  - Altra novità del recente provvedimento riguarda i trattamenti di dati effettuati tramite sistemi di videosorveglianza **direttamente collegati con le forze di polizia**. In questo caso, infatti, il Garante ha previsto un apposito modello semplificato di informativa "minima" indicante il titolare del trattamento, le finalità perseguite e il collegamento con le forze di polizia.

La videosorveglianza

Principi da rispettare:

- **Informativa**
  - Il datore di lavoro ha un duplice obbligo di informativa:
    - Da un lato deve predisporre e pubblicizzare una **policy interna** rispetto agli usi ed agli eventuali controlli, unitamente ad una idonea informativa ai dipendenti circa il sistema di videosorveglianza installato;
    - Dall'altro deve provvedere ad informare tutti gli interessati ai sensi dell'articolo 13 del Codice in materia di protezione dei dati personali.
  - L'informativa attraverso il modello semplificato deve sempre essere integrata da un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1 del Codice.
  - Il Garante prescrive, altresì, che il titolare dia un'idonea informativa anche oralmente a chiunque ne faccia richiesta.

La videosorveglianza

Principi da rispettare:

- **Consenso**
  - In caso di impiego di strumenti di videosorveglianza da parte di aziende private la possibilità di raccogliere lecitamente il consenso può risultare di difficile applicazione.
  - Pertanto, il Garante, dando attuazione all'istituto del bilanciamento degli interessi, ha individuato i casi in cui è possibile installare telecamere senza il consenso degli interessati quando chi intende rilevare le immagini deve perseguire un interesse legittimo attraverso la raccolta di mezzi di prova o nell'intento di perseguire fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, finalità di prevenzione di incendi o di sicurezza del lavoro ecc.

La videosorveglianza

Principi da rispettare:

- **Verifica preliminare:**
  - è obbligatorio sottoporre i sistemi di videosorveglianza alla verifica preliminare del Garante quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare. Tra queste ipotesi il Garante ricomprende espressamente alcune tipologie di sistemi di videosorveglianza, quali:
    - i sistemi di raccolta delle immagini associati a dati biometrici;

La videosorveglianza

- **Principi da rispettare**:
  - **Verifica preliminare:**
    - I sistemi dotati di software che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima;
    - I sistemi c.d. "intelligenti", che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli;

La videosorveglianza

Principi da rispettare:

- **Verifica preliminare:**
  - I sistemi integrati nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nel punto 4.6. del Provvedimento(che disciplina i sistemi integrati di videosorveglianza);
  - I sistemi per i quali si ritenga debbano essere previsti tempi di conservazione dei dati maggiori di sette giorni, a meno che non vi sia una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria;
  - I sistemi che prevedano trattamenti che abbiano natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel Provvedimento non sono integralmente applicabili.

La videosorveglianza

Principi da rispettare:

- **Accesso ai dati:**
  - Devono essere nominati per iscritto Incaricati del trattamento:
    - le persone fisiche autorizzate ad accedere ai locali dove sono situate le postazioni di controllo;
    - le persone fisiche autorizzate ad utilizzare gli impianti;
    - le persone fisiche autorizzate a visionare le immagini.
  - Deve trattarsi di un numero delimitato di soggetti, in particolare quando il titolare si avvale di una collaborazione esterna.
  - I dati devono essere protetti da idonee misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito.

La videosorveglianza

Principi da rispettare:

- **Periodo di conservazione dei dati**
  - In caso di registrazione, il periodo di conservazione delle immagini deve essere limitato a **poche ore o al massimo 24 ore**, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini. Per attività particolarmente rischiose (es. banche) è ammesso un tempo più ampio, che non può superare comunque la settimana.

  - Il sistema impiegato deve essere programmato **in modo da operare al momento prefissato - ove tecnicamente possibile - la cancellazione automatica da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.**

- **CONTROLLI A DISTANZA SUL LAVORATORE:**
  posta elettronica, navigazione internet e social network.

Le Linee Guida del Garante

- In questo contesto si inserisce il provvedimento del Garante della protezione dei dati personali del 1 marzo 2007 contenente le **“linee guida in materia di controllo da parte del datore di lavoro sull’utilizzo di internet e della posta elettronica da parte dei dipendenti”**

- La ragione principale dell’emanazione di un tale provvedimento è stata la ricezione da parte dell’autorità Garante di numerosi reclami, segnalazioni e quesiti riguardanti il trattamento dei dati personali effettuati dai datori di lavoro in relazione all’utilizzo di internet e della posta elettronica aziendali e i conseguenti poteri di controllo sui dati e più in generale le informazioni raccolte dal sistema informativo aziendale

- Si tratta di un provvedimento che, seppur circoscritto ai controlli sull’utilizzo di internet e della posta elettronica delinea alcuni principi che possono essere applicati analogicamente anche ad altre tipologie di controllo

Le Linee Guida del Garante

I principi generali

I principi generali del Codice in materia di protezione dei dati personali	
Principio di necessità	I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice)
Principio di correttezza	Le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati
Principio di pertinenza e non eccedenza	I trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile". Le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"

Le Linee Guida del Garante

Controlli e correttezza nel trattamento

- Ai fini del rispetto del **principio di correttezza**, l'eventuale trattamento da parte del datore di lavoro di dati personali relativi all'attività di controllo su internet e posta elettronica, **deve essere ispirato ad un canone di trasparenza, come tra l'altro previsto dall'articolo 4 dello Statuto dei Lavoratori**

- **Grava quindi sul datore di lavoro l'onere di indicare** in ogni caso, chiaramente e in modo particolareggiato, **quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli**. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali

- Le Linee Guida prospettano che il datore di lavoro **adotti un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente** (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) **e da sottoporre ad aggiornamento periodico**

Le Linee Guida del Garante.

Controlli e correttezza nel trattamento

- All'onere per il datore di lavoro di predisporre e pubblicizzare una policy interna rispetto agli usi ed agli eventuali controlli, si affianca il **dovere di informare comunque gli interessati (lavoratori) ai sensi dell'articolo 13 del Codice in materia di protezione dei dati personali**

- Con riferimento alle finalità perseguite, occorre indicare nell'informativa che i dati personali verranno raccolti e trattati per ragioni connesse a specifiche esigenze organizzative, produttive e di sicurezza sul lavoro quando comportano un trattamento lecito di dati e possono anche riguardare l'esercizio di un diritto in sede giudiziaria

Le Linee Guida del Garante
Apparecchiature preordinate al controllo a distanza

Divieti di cui all'art. 4 Statuto dei Lavoratori
Apparecchiature che consentono 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
Apparecchiature che consentono la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore
Apparecchiature che consentono la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo
Apparecchiature che consentono l'analisi occulta di computer portatili affidati in uso

Le Linee Guida del Garante

Apparecchiature preordinate al controllo a distanza

- Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro
- A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili

Le Linee Guida del Garante

La navigazione web

Misure preventive datoriali
Individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa
Configurazione dei sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato)
Trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai fil di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori)
Eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza

Le Linee Guida del Garante

La posta elettronica

Misure preventive datoriali
Rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali
Valutare la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore
Mettere a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. E' opportuno inoltre prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati.

Le Linee Guida del Garante

La posta elettronica

Misure preventive datoriali
In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, fare in modo che l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile
Fare in modo che i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale

Le Linee guida del Garante

I principi di pertinenza e non eccedenza dei controlli

Graduazione dei controlli

- **Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata**
- **L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.**
- Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Le Linee guida del Garante

I principi di pertinenza e non eccedenza dei controlli

Graduazione dei controlli

- **Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.**
- **Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.**
- Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Le Linee guida del Garante

I principi di pertinenza e non eccedenza dei controlli

Conservazione

- **I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) 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 deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario (e predeterminato) a raggiungerla

Le Linee guida del Garante

I principi di pertinenza e non eccedenza dei controlli

Conservazione

- **Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo 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 o della polizia giudiziaria.
- In questi casi, il trattamento dei dati personali deve essere 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 già esplicitati.

Le Linee guida del Garante

Presupposti di liceità del trattamento: bilanciamento di interessi

Datori di lavoro privati

- I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (*v., in particolare, art. 4, secondo comma, dello Statuto*), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili
- Ciò, può avvenire:
  - a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*)
  - b) in caso di valida manifestazione di un libero consenso
  - c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*)

Le Linee guida del Garante

Presupposti di liceità del trattamento: bilanciamento di interessi

Datori di lavoro privati

- **Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro)**
- L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26)

Grazie per l'attenzione

Maria Cristina Daga
mariacristina.daga@p4i.it