DISCIPLINARE PER GLI AUTORIZZATI AL TRATTAMENTO DEI DATI DELL'AZIENDA SPECIALE BERGAMO SVILUPPO

1. Premessa

Con il Regolamento (UE) n. 679/2016 (di seguito, anche "GDPR"), di fondamentale importanza è diventata l'organizzazione dei ruoli e dei rispettivi compiti in materia di trattamento dei dati e riservatezza.
In particolare, è possibile procedere alla individuazione e nomina dei Responsabili esterni, del Referente del Titolare, dei Referenti interni e, ancorché non espressamente previsto dal GDPR, anche degli Autorizzati al Trattamento dei dati personali per conto del Titolare o del Responsabile.
In questo ultimo caso, il Garante Privacy ha sottolineato l'opportunità che Titolare e Responsabili mantengano in essere la struttura organizzativa e le modalità di designazione degli Autorizzati al Trattamento così come delineate negli anni, anche attraverso gli interventi del Garante stesso.

2. Linee operative

A prescindere dai diversi ruoli aziendali in materia di Privacy si può convenire che tutti il personale dell'Azienda risulta comunque Autorizzato al trattamento dei dati di propria competenza.

Il personale autorizzato di un trattamento di dati personali deve operare in modo tale che vengano rispettate le normative vigenti per la riservatezza dei dati e la sicurezza del trattamento e deve seguire le disposizioni particolari fissate dal proprio Referente interno.

Le norme di comportamento standard adottate dell'Azienda per i trattamenti di dati personali sono riportate, oltre che nel presente disciplinare, "Piano generale per la sicurezza dei documenti" disponibile nella rete aziendale comune ed il rispetto delle indicazioni ivi contenute è tassativo. Per qualsiasi altra informazione o dubbio è sempre possibile rivolgersi al Referente privacy interno o al DPO aziendale.

Di seguito sono descritte le modalità con cui i dati devono essere trattati al fine di essere allineati con la normativa dettata dal Regolamento UE GDPR (2016/679) le quali presentano alcune variazioni a secondo della tipologia di dati trattati: solo dati Comuni, Particolari (ex Sensibili) e Giudiziari.

2.1. Trattamento di dati personali comuni (artt. 5 e seguenti GDPR)

L'autorizzato opera in modo tale che i dati personali comuni oggetto di trattamento siano:

1. trattati in modo lecito, corretto e trasparente nel confronti dell'Interessato ("*liceità, correttezza e trasparenza*";
2. raccolti e registrati per scopi documentati e determinati, espliciti e legittimi, ed utilizzati in altri trattamenti correlati in modo compatibile con gli scopi per cui sono stati raccolti ("*limitazione delle finalità*");
3. esatti e, se necessario, aggiornati; devono essere, inoltre, adottate tutte le ragionevoli misure per la cancellazione o la rettifica tempestiva dei dati inesatti, rispetto alle finalità del trattamento ("*esattezza*");
4. adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o

successivamente trattati ("*minimizzazione dei dati*");
5. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. I dati personali possono comunque essere conservati per periodi di tempo più lungo, a condizione che siano trattati esclusivamente ad archiviazione per pubblico interesse, ricerca scientifica o storica e fini statistici ("*limitazione della conservazione*");
6. trattati in maniera da garantire un'adeguata sicurezza dei dati personali - compresa la protezione mediante misure tecniche ed organizzative adeguate – da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale ("*integrità e riservatezza*").

Ai sensi degli artt. 32 e seguenti del GDPR, le attività di trattamento devono seguire le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare – su base permanente – riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali, in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza nel trattamento.

In attuazione delle previsioni di legge gli autorizzati devono:

a) utilizzare l'autenticazione informatica, custodendo con la massima riservatezza le credenziali di accesso e le passwords; le credenziali non possono essere comunicate a terzi e non possono essere custodite in chiaro; le password devono essere cambiate almeno ogni sei mesi (tre mesi in caso di trattamenti di dati particolari e giudiziari);
b) eseguire esclusivamente i trattamenti funzionali o strumentali all'esecuzione dei compiti loro attribuiti e raccogliere e trattare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere tali compiti;
c) fornire all'interessato l'informativa di cui all'articolo art. 13 del Regolamento UE GDPR (2016/679) così come predisposta e resa disponibile;
d) comunicare a terzi i dati personali solo nei casi espressamente previsti da legge o da regolamento e non utilizzare per altri fini i dati personali di cui dovessero venire a conoscenza nell'esecuzione delle operazioni suddette e comunque mantenere la più completa riservatezza sui dati trattati e sulle tipologie di trattamento effettuate. Tali obblighi sono da considerarsi pienamente vigenti anche nel caso di cessazione del rapporto di lavoro;
e) attivare la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) seguire le indicazioni del Referente privacy interno comunicate durante le attività di formazione o nei vari disciplinari operativi;
g) accedere ai soli dati personali strettamente necessari per compiere il trattamento loro assegnato e conservare gli atti e i documenti contenenti i dati per il tempo occorrente - con riferimento ai termini di legge o regolamentari – al trattamento e reinserirli negli archivi a conclusione delle operazioni affidate.

Nel caso in cui il trattamento sia effettuato con supporti cartacei o richieda supporti cartacei si

deve prevedere:

h) idonea custodia di atti e documenti affidati agli autorizzati per lo svolgimento dei relativi compiti e loro restituzione al termine delle operazioni affidate;
i) conservazione di determinati atti in archivi ad accesso selezionato;

Per attuare idonea custodia agli uffici e agli archivi di trattamento si possono adottare le seguenti semplici precauzioni:

j) chiudere a chiave la porta di accesso agli uffici in assenza del personale preposto;
k) mantenere la documentazione cartacea negli armadi;
l) mantenere la massima riservatezza con gli estranei e prestare la massima attenzione a comportamenti di personale non addetto.

Nel valutare l'adeguato livello di sicurezza, si deve in particolar modo tener conto dei rischi presentati dal trattamento dei dati, soprattutto dalla loro distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso – in modo accidentale e/o illegale – ai dati personali trasmessi, conservati o trattati.
In caso di violazione delle normative e delle regole, l'autorizzato deve informare tempestivamente il Referente interno e seguire le eventuali indicazioni che egli darà per minimizzare le ricadute sull'azienda.

Va ricordato che ai sensi degli artt. 33 e seguenti del Regolamento, in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di Controllo competente, senza ingiustificato ritardo e, se possibile, entro le successive 72 ore dalla venuta a conoscenza.
Inoltre, quando la violazione dei dati personali è suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'Interessato senza ritardo ingiustificato.

2.2. Trattamento di dati personali particolari (ex sensibili per la 196/2003) (artt. 9 e seguenti GDPR)

Il Regolamento UE n. 679/2016 sancisce il divieto di trattamento di dati "*personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*". Il generale divieto di trattamento di detti dati, non opera nel caso in cui:

- l'interessato abbia prestato il proprio consenso esplicito al trattamento dei dati personali, per una o più finalità specifiche;
- il trattamento sia necessario per assolvere gli obblighi ed esercitare diritti specifici del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro, sicurezza sociale e protezione sociale, in presenza comunque di garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato;
- 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, ex membri o persone che hanno regolari contatti e che i dati personali non siano comunicati all'esterno senza il consenso dell'Interessato;
- il trattamento sia necessario per tutelare un interesse vitale dell'Interessato o di altra persona fisica, nel caso in cui il primo si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento riguardi dati personali resi manifestamente pubblici dall'Interessato stesso;
- il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento sia necessario per motivi di pubblico interesse rilevante, che deve essere proporzionato rispetto alla finalità perseguita, nel rispetto dell'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato;
- il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, per la valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, ovvero gestione dei sistemi e servizi sanitari o sociali, fatti salvi i casi in cui i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza;
- il trattamento sia necessario per motivi di interesse pubblico nel settore della Sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
- il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sia proporzionato alla finalità eseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'individuo.

L'Autorizzato al trattamento <u>di dati personali particolari</u> opererà nelle seguenti modalità:

m) nel momento in cui i dati particolari sono (come nella maggioranza dei casi) relativi ai dipendenti dell'Azienda e quindi legati alla gestione del Personale, ove si trattino dati storici compresi eventuali file di pertinenza dell'interessato, devono essere conservati in un archivio informatico riservato dell'Ufficio Amministrazione opportunamente autorizzato;
n) nel caso in cui il trattamento sia effettuato con supporti cartacei o richieda supporti cartacei si deve attuare idonea custodia tramite conservazione di quei determinati documenti (o atti) contenenti dati particolari, in archivi ad accesso selezionato o chiuso o in un ufficio presidiato, o in un armadio/cassetto dotato di serratura con chiave; quest'ultima affidata in custodia all'incaricato del trattamento autorizzato;
o) i supporti contenenti dati particolari devono, se possibile, essere marcati con un'opportuna etichetta recante la dicitura "Contiene dati personali particolari (ex sensibili per la 196/2003) artt. 9 e seguenti GDPR) Rispettare quanto previsto dal trattamento";
p) è vietato produrre copie anche parziali dei documenti contenenti dati sensibili salvo diverse esplicite disposizioni relative a procedure per cui le copie sono indispensabili; tutte le copie vengono trattate con le stesse misure di riservatezza e sicurezza degli originali e distrutte dopo l'uso dallo stesso incaricato al trattamento dei dati contenuti;
q) la stampa dei documenti contenenti dati particolari deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato del trattamento. Detti documenti

vanno eliminati, quando non sia più necessario conservarli per gli scopi per cui sono stati stampati;

Tenuto conto dei particolari limiti e garanzie che il Regolamento Ue n. 679/2016 prevede, l'Autorizzato è tenuto al compimento delle attività di trattamento nel pieno rispetto della normativa vigente e soprattutto delle peculiarità previste - ai sensi dell'art. 9 del GDPR – per i dati personali particolari.

2.3. Trattamento di dati personali relativi a condanne penali e reati

Con specifico riguardo al trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, ai sensi dell'art. 10 del Regolamento UE n. 679/2016, esso "*deve avvenire soltanto sotto il controllo dell'Autorità Pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dagli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica*".

Per la natura dei dati trattati di tipo giudiziario, l'attenzione da prestare sul trattamento dei dati stessi in relazione al tema Privacy, normato dal Regolamento UE GDPR (2016(679), deve essere molto puntuale, mantenendo la massima riservatezza nello svolgimento delle attività e nella custodia di tali informazioni, siano esse in forma elettronica siano in forma cartacea.

Data la particolarità dei dati trattati si precisa:

- il divieto di apertura di buste contenenti atti giudiziari, se non in ottemperanza alle disposizioni ricevute e per lo svolgimento del proprio compito lavorativo
- l'obbligo di segretezza
- il divieto di stampare documenti contenenti dati giudiziari, salvo particolari esigenze d'ufficio, in tal caso la stampa deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato del trattamento
- la loro eliminazione, quando non sia più necessario conservarli per gli scopi per cui sono stati stampati;
- il cambio delle password di accesso ai sistemi ogni tre mesi.

Ogni accesso e/o comunicazione e/o diffusione di dati verso soggetti esterni dovrà essere autorizzato preventivamente dal Referenti interno.