24 POLICY ENTE PER TRATTAMENTI SU SUPPORTI ELETTRONICI e CARTACEI

documento da mettere a disposizione delle persone fisiche (incaricati, responsabili, custodi password, responsabili aree ad accesso limitato, ecc) che, a fronte della lettera di incarico firmata, debbano mantenersi aggiornati e prendere coscienza dell'elenco aggiornato delle misure minime attuate dall'Ente

24.1 Principi del presente documento.

Il Dlgs. 30 giugno 2003 n° 196, pubblicato in Gazzetta Ufficiale il 29 luglio 2003, ha introdotto il Testo Unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, la cui entrata in vigore è stata fissata al 1° gennaio 2004.

Il codice ha codificato il principio secondo il quale chiunque ha diritto alla protezione dei propri dati personali.
La privacy si configura quale il diritto a mantenere il controllo sulle informazioni relative alla propria persona e sull'uso che di esse viene da altri fatto.

L'evoluzione normativa giunge ad una svolta con il vaglio del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016.
La normativa europea ha ad oggetto la protezione delle sole persone fisiche con riguardo al trattamento dei dati personali.
L'efficacia diretta del regolamento europeo ha comportato l'entrata in vigore del testo di legge nel nostro ordinamento senza bisogno di una legge interna di recepimento; tuttavia, le istituzioni europee hanno differito l'entrata in vigore dell'apparato sanzionatorio del regolamento fino al 25 maggio 2018 permettendo così a soggetti pubblici e privati di adeguarsi alla normativa.

Nell'intento di raggiungere la massima chiarezza concettuale ed applicativa, il regolamento generale sulla protezione dei dati (RGDP) espone nel suo art.4 le principali definizioni in materia di trattamento dei dati personali, descrivendo il trattamento come "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

Il regolamento disciplina i soggetti, i mezzi, le limitazioni nonché le violazioni al trattamento di dati personali; violazioni alle quali è connesso un articolato quadro sanzionatorio connotato da illeciti amministrativi e pene pecuniarie fino a 20 milioni di euro.

Il panorama normativo italiano risulta così radicalmente mutato.
La pubblicazione del Dlgs. 101/2018 il 4 settembre 2018, entrato in vigore il 19 settembre 2018, sancisce dunque l'adeguamento del Dlgs. 196/2003 al regolamento europeo.
In particolare l'art. 2 specifica: "*Il presente Codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento*".

Il Dlgs 101/2018 introduce un sistema sanzionatorio di rilevanza penale (artt. 167 ss) nell'ottica di rendere maggiormente effettiva e deterrente la normativa in materia di protezione di dati personali, con pene che vanno dall'arresto alla reclusione fino a sei anni.

La preoccupazione di fondo del legislatore italiano ed europeo è quella di impedire che, grazie ad una tecnologia sempre più avanzata, vengano raccolte in database al fine di un uso distorsivo quante più informazioni possibili sugli individui (dalla religione di appartenenza alla marca di pasta acquistata nel supermercato).

La sicurezza del trattamento assurge a chiave di lettura della legittimità del trattamento, ed in tal senso l'art. 32 RGDP prevede altresì la redazione di un'analisi dei rischi incombenti sui dati: "*Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*".
Detta analisi viene trascritta in un documento redatto a cura del titolare del trattamento dei dati personali (sotto forma di archivi elettronici o cartacei).

A coadiuvare gli operatori economici nell'applicazione del nuovo quadro normativo costituito dal regolamento UE e dal Dlgs. 196/2003, così come novellato dal Dlgs. 101/2018, saranno le attese linee guida del Garante per la Protezione dei dati Personali, il quale guiderà i soggetti destinatari della normativa nel compimento dei dovuti adempimenti di modo da risultare privacy compliant.

Approfondimenti sul GDPR.
Il GDPR ha introdotto un nuovo concetto: **l'accountability** ovvero la **responsabilizzazione** che, insieme alla **consapevolezza**, sono gli elementi di novità introdotti con il Regolamento. Il Titolare del trattamento non ha più misure impartite dal testo normativo identificanti le modalità di trattamento ma, al contrario, è l'unico soggetto detenente la responsabilità sui dati lui affidati dagli interessati (o da titolari terzi nel caso in cui operi come Responsabile).
Ne consegue che le misure sono da identificarsi a cura del Titolare e sono tutte le misure che un "buon padre di famiglia" adotterebbe per tutelare quanto gli è più caro.

Ulteriore elemento di primaria importanza è la consapevolezza, con particolare riferimento alla consapevolezza della governance aziendale: senza consapevolezza e responsabilizzazione nessuna misura può essere posta efficacemente a tutela dei dati personali trattati dal Titolare.

Il trattamento dei dati personali richiede obbligatoriamente il rispetto delle prescrizioni indicate nel Regolamento stesso nonché l'adozione di idonee e preventive misure di sicurezza: **chiunque essendovi tenuto omette di adottare quanto previsto dal Regolamento è suscettibile di sanzioni in sede penali ed in sede civili**. Le misure di sicurezza prescritte dal "Codice" sono intese nel senso più ampio e riguardano il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano i livelli di protezione necessari a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nell'ambito del più generale quadro degli obblighi di sicurezza, il "Codice" prescrive in modo specifico le misure che debbono comunque essere adottate per assicurare un livello minimo di protezione dei dati personali, rinviando al "Disciplinare tecnico" per le modalità della loro applicazione.

In ottemperanza agli obblighi di legge viene emesso il presente documento che integra ogni eventuale precedente normativa interna al riguardo.
Tutto il personale dipendente, compresi gli stagisti ed i lavoratori interinali, dipendenti distaccati da altre aziende partecipate/controllate assegnati ad unità operative interne, i consulenti di aziende esterne o collaboratori autonomi, gli addetti alla manutenzione SW, gli addetti alla

sostituzione e manutenzione dei dischi e altro HW sono tenuti a rispettarlo scrupolosamente, nell'ambito delle proprie competenze ed attività.

Inosservanza delle disposizioni riportate a seguire da parte delle risorse umane dell'Ente.
La violazione , parziale o totale, delle disposizioni riportate a seguire, potrà essere suscettibile di provvedimenti disciplinari commisurati alla gravità della violazione. Si raccomanda pertanto ai destinatari del presente documento di ottemperare alle indicazioni di seguito enunciate e di completare la compilazione del documento siglando lo stesso "per ricevuta e presa visione ed accettazione ".

Obbligo di riservatezza.
Gli incaricati, nel trattare i dati personali, dovranno operare garantendo la massima riservatezza delle informazioni di cui vengono in possesso, considerando tutti i dati personali confidenziali e, di norma, soggetti al segreto d'ufficio.

24.2 Applicabilità.

Il presente Documento Unico Rispondenza Privacy si applica a tutti gli elaboratori elettronici, tutte le sedi, tutti i locali, tutti gli incaricati, responsabili, titolari del trattamento ed a tutto il personale coinvolto, a vario titolo, nelle sessioni di trattamento dati effettuati per nome e conto dell'Ente:
PANIFICIO PASTICCERIA TOSSINI 1 S.P.A. anche qualora questa operi in qualità di Responsabile esterno al trattamento per conto terzi.

24.3 Revisione e validità del presente documento.

Il presente documento è valido fino a quando gli elementi dell'Ente che intervengono durante il corso del trattamento dei dati non subiscono variazioni.
Nel momento in cui uno o più elementi subissero variazioni, il presente documento dovrà essere immediatamente aggiornato quindi ristampato e portato a conoscenza del personale.

Gli aggiornamenti terranno presente anche i livelli di rischio a cui sono soggetti i dati personali, sensibili, giudiziari nonché eventuali modifiche della tecnologia informatica.

24.4 Definizioni.

Relativamente al presente documento si intende per:

1. Ente, l'insieme di persone e cose costituito da PANIFICIO PASTICCERIA TOSSINI 1 S.P.A.

Definizioni ai fini del GDPR 2016/679 s'intende per:

1. "**dato personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o piu' elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2. "**trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3. "**titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

4. "**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

5. "**responsabile della protezione dei dati**" o "DPO": soggetto designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti specifici previsti dall'articolo 39; il DPO dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

6. "**destinatario**": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

7. "**terzo**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

8. "**dati genetici**": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

9. "**dati biometrici**": i 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;

10. "**dati relativi alla salute**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

11. "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

12. "**profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

13. "**pseudonimizzazione**": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

14. "**archivio**": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

15. "**stabilimento principale**":
    a. per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    b. con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione

centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

16. "**rappresentante**": la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

17. "**impresa**": la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

18. "**gruppo imprenditoriale**": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

19. "**norme vincolanti d'impresa**": le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

20. "**autorità di controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

21. "**autorità di controllo interessata**": un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
    b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
    c. un reclamo è stato proposto a tale autorità di controllo;

22. "**trattamento transfrontaliero**":
    a. trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
    b. trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

23. "**obiezione pertinente e motivata**": un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

24. "**servizio della società dell'informazione**": il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

25. "**organizzazione internazionale**": un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Intelligenza artificiale - Artificial Intelligence (AI)

L'Intelligenza Artificiale (IA) è una tecnologia che permette a sistemi e software di eseguire attività che normalmente richiederebbero l'intelligenza umana, come l'apprendimento, la risoluzione di problemi, il riconoscimento di modelli e la comprensione del linguaggio naturale. L'IA può supportare il lavoratore automatizzando compiti ripetitivi, migliorando l'efficienza operativa e offrendo analisi avanzate per prendere decisioni informate. Più in generale, può migliorare la qualità della vita delle persone, facilitando l'accesso a servizi personalizzati, aumentando la sicurezza e rendendo più efficienti le attività quotidiane.

Articolo 29

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento.

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

Ulteriori termini utilizzati nel presente documento:

"**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

"**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

"**interessato**", la persona fisica cui si riferiscono i dati personali

"**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Ai fini del GDPR si intende, inoltre, per:

«**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«**consenso dell'interessato**»: qualsiasi manifestazione di volontà **libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
inequivocabile è per iscritto o se si da luogo al contratto sottoscritto per beni e servizi

«**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

«**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

24.5 Attribuzione degli incarichi.

Titolare del trattamento.
I seguenti soggetti sono coloro che rivestono la carica di Titolare del trattamento dati:

Non essendo stato indicato un Titolare del trattamento, l'Ente stessa verrà considerata a tutti gli effetti come Titolare dei trattamenti.

Responsabile del trattamento, interni alla struttura del titolare.
I seguenti soggetti sono coloro che rivestono la carica di Responsabile del trattamento dati:

Non sono state indicati soggetti che ricoprano i sopracitati incarichi

Soggetti che operanti sessioni di trattamento per nome e conto del titolare.

Estremi identificativi	Posizione nell'Ente	Posizione nel trattamento dati
GRUPPO OMOGENEO ADDETTI PRODUZIONE	Addetti alla produzione industriale	incaricato trattamento
GRUPPO OMOGENEO REPARTO OFFICINA	Addetti alla manutenzione macchine	incaricato trattamento
GRUPPO OMOGENEO MAGAZZINIERI	Magazziniere	incaricato trattamento
GRUPPO OMOGENEO ADDETTI AL CONFEZIONAMENTO	Addetti al confezionamento	incaricato trattamento
DANIELE AGATI	Impiegato Commerciale	incaricato trattamento
Roberto Arboccò	Responsabile stabilimento	incaricato trattamento
CHIARA CARRARA	Responsabile Commerciale e Marketing	incaricato trattamento
IGOR CLIVIO	Apprendista ufficio programmazione produzione	incaricato trattamento
Adriano Lucchesi	Responsabile produzione	incaricato trattamento
SABRINA MARTINELLI	Responsabile Qualità	incaricato trattamento
LUCA MELE	Impiegato Ufficio Acquisti	incaricato trattamento
Jesus Miguel Osuna Di Tomo	Adetto programmazione produzione	incaricato trattamento
ROMINA PICASSO	Impiegata logistica e ordini	incaricato trattamento
ALESSIO ROSSI	Responsabile Logistica	incaricato trattamento
Ermes Schinca	Socio	incaricato trattamento
ANTONIO SORACCHI	Responsabile Officina	incaricato trattamento
Maurizio Tossini	Membro del Consiglio di Amministrazione	incaricato trattamento
CLAUDIO VIVONA	Responsabile controllo gestione	incaricato trattamento
Mara Bertuccio	Ufficio Qualità	incaricato trattamento insourcing
CRISTINA CASCIO	Impiegata ufficio logistica	incaricato trattamento insourcing
Manuela Chiefa	Impiegata commerciale	incaricato trattamento insourcing
Giorgia D'Ostuni	Membro del Consiglio di Amministrazione - Responsabile compliance - Gestore delle segnalazioni	incaricato trattamento insourcing
outsourcing | Savino Dr. Gianluca	Commercialista	incaricato trattamento outsourcing
outsourcing | Fratelli Tossini Srl	Responsabile amministrativo/contabile	incaricato trattamento outsourcing
outsourcing | Studio Peroni	Consulente legge 81/08	incaricato trattamento outsourcing
outsourcing | Abbene Alessio	Consulente legale	incaricato trattamento outsourcing
outsourcing | Project Consult Srls	Consulente privacy	incaricato trattamento outsourcing

Personale che può venire in contatto sporadicamente con i dati trattati.
I seguenti soggetti, a fronte delle mansioni svolte per l'Ente, possono sporadicamente entrare in contatto e/o visionare i dati trattati sia in forma elettronica che in forma cartacea:

Non sono state indicate persone fisiche che ricoprano i sopracitati incarichi

Personale tecnico.
I seguenti soggetti, a fronte delle mansioni svolte per l'Ente, sono indicati come personale tecnico o come custodi delle credenziali elettroniche.

Estremi identificativi	Posizione nell'Ente	Posizione nel trattamento dati
outsourcing | I VIGILI DELL'ORDINE	Sistemi e servizi di vigilanza privata	amministratore di database
DANIELE DEL MASTRO	Amministratore di sistema	amministratore di sistema
Mino Ganzerli	Amministratore di sistema	amministratore di sistema

24.6 Mansioni attribuite e tempistica di applicazione.

"I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."

Titolare del trattamento.

è onere del Titolare del trattamento dati verificare costantemente che le misure minime di sicurezza siano rispettate sia in regime di trattamenti dati svolti in seno all'Ente che in regime di trattamenti dati svolti presso aziende esterne (outsourcing).
Tale compito non è demandabile;
è fatto obbligo all'Ente la tenuta di un aggiornato Documento Unico Rispondenza Privacy : tale mansione potrà essere espletata in concerto con il/i Responsabile/i del trattamento, il consulente in materia di trattamento di dati ed il Responsabile della Protezione dei dati (DPO);
è onere del Titolare del trattamento dati ottenere, nel caso di installazioni effettuate da soggetti esterni all'Ente, la dichiarazione che le installazioni siano state effettuate nel rispetto della normativa vigente. Tale compito può essere demandato al Responsabile del trattamento.
è onere del Titolare del trattamento dati adoperarsi affinchè, nel caso in cui l'Ente tratti i dati sensibili o giudiziari, venga implementato un sistema per la protezione dei locali rilevanti per detti trattamenti;
Detto sistema dovrà prevedere anche il monitoraggio degli accessi, degli incaricati del trattamento dei dati sensibili o giudiziari, soprattutto dopo l'orario di lavoro. Tale compito può essere demandato al Responsabile del trattamento.

Responsabile del trattamento.

Il Responsabile al trattamento è, secondo l'accezione del GDPR, un soggetto esterno alla struttura (libero professionista, società, etc.).

Il Responsabile del trattamento ha l'obbligo in senso generale di ottemperare al perseguimento delle finalità stabilite dal Titolare, trattando i dati secondo le istruzioni e modalità di trattamento impartite dal Titolare stesso, nonché di verificare che le misure di sicurezza vengano applicate e di informare prontamente il Titolare in casi di situazioni anomale o di accessi abusivi ai dati.

Nel caso in cui vi sia contratto - o documento equivalente a norma del diritto dello stato membro - tra il Titolare ed il Responsabile, riportante la descrizione analitica dei compiti e riportante le attività a lui attribuite, il Responsabile avrà l'onere di implementare, monitorare, gestire unicamente i compiti a lui affidati per iscritto.
Laddove i Responsabili del trattamento eletti siano più di uno, le sotto menzionate attività saranno affidate a ciascuno in funzione dei propri compiti assegnati per iscritto, a mezzo di apposito contratto, ed elencati analiticamente.

24.7 INDICAZIONE ANALITICA COMPITI AFFIDATI

(a responsabili ed incaricati al trattamento)

24.7.1 ID: 180

TITOLO: Risorse Umane, Clienti, Fornitori
DESCRIZIONE: ATTIVITÀ STRUMENTALI PER LA RICEZIONE E GESTIONE DELLA SEGNALAZIONE

ID:
TITOLO:
DESCRIZIONE:

24.7.2 Misure di carattere generale.

In carenza di indicazione specifica fare riferimento alle seguenti indicazioni.

1) **Autenticazione informatica**: l'Ente verificato periodicamente il corretto funzionamento del sistema di autenticazione informatica, direttamente o indirettamente attraverso aziende specializzate, provvede ad adottare le opportune azioni tendenti a manutenere detta procedura di autenticazione, l'eventuale ripristino, se necessario, del sistema di autenticazione informatica.

2) **Attribuzione delle credenziali elettroniche**: ogni qualvolta un incaricato viene autorizzato ad operare in nuovi ambiti di trattamento dati, l'Ente attribuisce una username univoca ed una password informando l'incaricato circa l'obbligo di modificare la password immediatamente dopo il primo utilizzo. L'Ente informa altresì l'incaricato circa la modalità di creazione della propria password ovvero il numero minimo di caratteri (8 o il numero massimo accettabile al sistema se inferiore ad 8), i caratteri contenuti nella password (non facilmente riconducibili al Titolare della credenziale elettronica e contenenti di caratteri numerici ed Alfanumerici).

3) **Verifica degli ambiti di trattamento**: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici con cadenza almeno annuale.

4) **Protezione degli strumenti elettronici e dei dati**: con particolare attenzione alle evoluzioni della tecnica, degli strumenti elettronici e dei software per la protezione degli strumenti elettronici ed i dati in essi contenuti, l'Ente dovrà verificare periodicamente (almeno semestralmente per elaboratori elettronici che trattano dati personali o almeno trimestralmente per elaboratori elettronici che trattino dati sensibili o giudiziari) che i sistemi software (a titolo esemplificativo, ma non esaustivo, antivirus, firewall, aggiornamenti del sistema operativo, ecc.) implementati nei vari elaboratori elettronici siano stati aggiornati.
è suggerito un aggiornamento più frequente rispetto a quello previsto dalla normativa vigente ovvero l'aggiornamento dei sistemi antivirus e del sistema operativo installato sui vari elaboratori elettronici dovrebbe essere effettuato ogni qualvolta gli aggiornamenti vengano resi disponibili dal produttore del software o del sistema operativo e in subordine il controllo circa la disponibilità di aggiornamenti dovrebbe essere effettuato ogni qualvolta l'elaboratore si connetta alla rete Internet.
è compito dell'Ente installare detti aggiornamenti su tutti gli elaboratori anche su quelli che non siano connessi direttamente ad Internet o che abbiano accesso ad Internet. è compito dell'Ente rendere informativa, scritta o orale, a tutti i gli incaricati ed al Titolare del trattamento circa la disponibilità di nuovi aggiornamenti relativi ai programmi di antivirus ed al sistema operativo dei vari elaboratori utilizzati nell'Ente per i trattamenti, unitamente a notizie relative a diffusione di virus informatici a livello locale, nazionale o mondiale ("pan-epidemie informatiche" ovvero diffusioni di virus informatici che sfruttino carenze di sicurezza di particolare gravità dei sistemi informatici).
Verrà, con tempistiche stabilite di volta in volta, posta in essere una verifica periodica della sicurezza dei sistemi informatici dell'Ente, accessibili o scollegati dalla rete pubblica di telecomunicazioni, effettuando una simulazione di attacco dall'esterno della propria rete locale, dall'interno della stessa e/o verificando lo stato delle varie porte di comunicazione degli elaboratori elettronici.

5) **Protezione dall'uso improprio degli strumenti elettronici**: è compito dell'Ente verificare che vengano ottemperate le norme stabilite dall'Ente in materia di uso improprio degli strumenti elettronici a disposizione degli incaricati. è suggerito che questa verifica sia estesa a tutti i dipendenti che abbiano accesso a strumenti elettronici anche se non incaricati del trattamento dati. A titolo esemplificativo, ma non esaustivo, file sharing (condivisione di file con altri utenti a mezzo connessioni point-to-point), scaricamento dalla rete Internet di file non autorizzati dall'Ente - contenuti in elenchi per tipologia o attività redatti per una specifica unità operativa o elenchi generali riguardanti l'intera attività svolta dall'Ente- , installazione a mezzo di CD-ROM o supporto equivalente, di programmi non espressamente autorizzati.

6) **Copie di sicurezza dei dati**: monitoraggio circa la creazione e/o la verifica di conformità delle copie di backup di vari dati con cadenza almeno settimanale, conservazione di dette copie nei locali adibiti dall'Ente per la loro conservazione. è suggerito che l'Ente verifichi, personalmente e/o attraverso apposita struttura, periodicamente la qualità di backup (verifica di creazione di copia conforme ai dati originari) e, nel caso di riutilizzo dei supporti riscrivibili, che la qualità dei supporti non sia stata ridotta in funzione del loro ripetuto utilizzo.
L'azienda esterna eletta dall'Ente per tale compito rilascia, al termine della prestazione richiesta, debita notula contenente un elenco delle operazioni effettuate, una descrizione delle memorie di massa oggetto della verifica, una dichiarazione di ottemperanza circa la normativa vigente allorchè tale evenienza sia verificata (backup idoneo al ripristino dei dati).
Le copie di sicurezza, se contenenti dati che comportano rischi per gli interessati, debbono essere oggetto di cifratura. È buona norma che qualsiasi copia di sicurezza dei dati sia cifrata preventivamente in modo da minimizzare i rischi di violazione d'accesso (data breach).

7) **Interventi formativi per il personale impiegato nel trattamento dei dati**: l'Ente verifica che tutti coloro che siano impiegati nel trattamento dati abbiano ricevuto gli interventi formativi previsti dalla normativa e dal piano di formazione allegato al DURP , tendenti a creare la consapevolezza, in dette persone, circa
- i rischi che incombono sui vari dati trattati nell'Ente,
- le misure per prevenire tali rischi,
- la normativa vigente in materia di trattamenti dati personali ed i profili di tale disciplina,
- modalità per aggiornarsi sulle misure di sicurezza adottate dall'Ente.

8) **Modalità di accesso a trattamenti dati performati esclusivamente da alcuni incaricati**: L'Ente, nel caso in cui un incaricato che acceda in maniera esclusiva ad un trattamento dati sia impossibilitato ad accedere al detto trattamento in tempi brevi (a titolo esemplificativo, ma non esaustivo, permessi per periodi di ferie presi dall'incaricato, periodi di assenza dall'Ente a causa di motivi di salute, ecc.), provvede alla redazione della modalità di accesso a detto trattamento. Tale modalità, da redigersi per iscritto, verrà conservata in busta chiusa in luoghi. Tale modalità comprenderà l'elenco delle persone in possesso delle credenziali elettroniche per accedere al trattamento. è suggerito un modello di comportamento che eviti la creazione ex novo delle credenziali elettroniche dell'incaricato avente accesso esclusivo a detto trattamento: a tal fine è suggerita la creazione di profili temporali che permettano l'accesso a detto trattamento, i quali verranno disattivati non appena l'incaricato sia nuovamente in grado di accedere al trattamento dati sopra indicato.

9) **Cifratura dei dati**: per i dati personali idonei a rivelare lo stato di salute, la vita sessuale, l'orientamento politico, religioso, filosofico di cui all'art. 9 del GDPR ovvero i dati relativi a condanne penali e misure di sicurezza ad essi connesse, l'Ente dovrà effettuare l'individuazione dei criteri, ed adozione degli stessi, per la cifratura e/o per la separazione di tali dati dai dati identificativi dell'interessato.

10) **Documento Unico Rispondenza Privacy** : è compito dell'Ente aggiornare (anche tramite strutture esterne come ad esempio consulenti, ditte specializzate, ecc.) la documentazione con cadenza almeno annuale o in funzione di significativi cambiamenti dell'asset di trattamento (incaricati, responsabili, dati trattati, strumenti elettronici, logistica, finalità di trattamento, titolarità del trattamento, eventi quali violazione

d'accesso ai dati - data breach, esercizio dei diritti da parte degli interessati).

11) **Politiche di riutilizzo memorie di massa**: laddove le memorie di massa siano oggetto di riutilizzo, è compito dell'Ente redigere, preventivamente a tale riutilizzo, la modalità (nonché la susseguente sua applicazione) affinchè i supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, siano distrutti o resi inutilizzabili, ovvero la possibilità di riutilizzare detti supporti allorchè le informazioni precedentemente in essi contenute siano rese non intelligibili e tecnicamente non ricostruibili in alcun modo.

12) **Ripristino dei dati e dei sistemi hardware e software**: è compito dell'Ente o, a fronte di apposita delega, del consulente, redigere le modalità per il ripristino degli elaboratori elettronici e dei dati in essi contenuti a fronte di eventi distruttivi che abbiano indifferentemente coinvolto gli uni che altri. Tale modalità comprende l'elencazione dei supporti di backup, la modalità con la quale gli stessi sono stati creati, l'elenco delle persone adibite al ripristino dei sistemi operativi, dei dati, la tempistica relativa al ripristino (numero di giorni necessari per ripristinare completamente i dati, in ogni caso non superiori a sette giorni nel caso in cui i dati trattati siano dati sensibili o giudiziari), le procedure e le modalità di ripristino e quant'altro possa facilitare il ritorno allo stato di fatto vigente prima dell'evento dannoso. Questa procedura tenderà a ristabilire lo stato di fatto di cui sopra entro tempi certi, compatibili con i diritti degli interessati ed indicati, ove presente, nel documento di disaster recovery.

13) **Cifratura dei dati**: è compito dell'Ente verificare che i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, siano trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente non intelligibili anche a chi sia autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.

14) **Aree ad accesso controllato**: nel caso in cui l'Ente tratti dati sensibili o giudiziari le aree preposte alla conservazione delle copie cartacee e/o dei supporti di backup nonché le aree di trattamento di detti dati, potranno essere accessibili solo dal personale autorizzato.
è compito dell'Ente creare tutti i presupposti affinchè tutti gli accessi durante il normale orario di lavoro siano effettuati unicamente dal personale autorizzato e che gli accessi dopo il normale orario di lavoro, effettuabili unicamente dal personale autorizzato, vengano monitorati;
è compito dell'Ente indicare per iscritto le persone autorizzate ad accedere alle aree riservate; tale attività viene espletata nel DURP allorchè vi sia l'elencazione delle postazioni di lavoro nonché la loro attribuzione ad uno o più soggetti;
è possibile che sia eletto un incaricato responsabile di area logistica il quale custodisca le chiavi dell'area ad accesso limitato a lui affidata, verifichi che le persone che accedono all'area siano effettivamente autorizzate ad accedervi, accompagni i visitatori occasionali, se autorizzati dall'Ente, controlli gli ingressi fuori dall'orario di lavoro (in subordine questa mansione è demandabile ad un sistema automatico di monitoraggio degli accessi fuori dall'orario di lavoro), verifichi l'efficacia degli allarmi attraverso l'esecuzione di periodici test.
Tali compiti sono delegati, in carenza di elezione del Responsabile d'area, al Responsabile della sede dell'Ente.

15) **Dispositivi mobili**: qualsiasi dispositivo mobile (ivi compresi smart phone e tablet) di proprietà dell'incaricato o dell'Ente non può accedere ai dati personali di cui l'Ente è il titolare a meno chè questo non sia esplicitamente approvato dall'Ente stessa. Il dispositivo dovrà essere sottoposto alla preventiva verifica ed alla approvazione dell'Ente e/o da parte del suo Amministratore di Sistema o equivalente personale tecnico. I dispositivi mobili dovranno essere oggetto di cifratura sia per la memoria interna che l'eventuale memoria estraibile, una password di accesso personale dovrà essere utilizzata per la loro apertura, il servizio di cancellazione, inizializzazione e reset del dispositivo da remoto ovvero l'impossibilità di aggirare tali funzioni dovrà essere attivata.

Incaricato del trattamento.

L'incaricato dovrà prestare particolare attenzione alle seguenti disposizioni oltre che ottemperare ai comportamenti di propria pertinenza indicati come a carico del Responsabile, nel precedente capitolo.

1) **Sostituzione password al primo accesso**: successivamente al primo accesso ad un qualsiasi trattamento dati, l'incaricato dovrà sostituire la componente privata delle credenziali elettroniche (password) redigendone una nuova composta da almeno otto caratteri (o il massimo accettabile da sistema di autenticazione se minore di otto caratteri), non contenente riferimenti facilmente riconducibili all'incaricato e contenente i caratteri numerici ed alfanumerici.

2) **Sostituzione della password**: l'incaricato ha l'obbligo di sostituire la propria password con cadenza semestrale o, nel caso di trattamento di dati sensibili o giudiziari, con cadenza trimestrale.

3) **Informazione circa la perdita delle qualità per un trattamento di dati**: incaricato dovrà informare il Responsabile, se presente, o in subordine il Titolare del trattamento dati, immediatamente dopo aver perso le qualità per l'accesso a determinati trattamenti di dati (articolo esemplificativo, ma non esaustivo, variazione delle mansioni dell'incaricato).

4) **Istruzioni circa la custodia degli elaboratori elettronici**: è compito dell'incaricato avere cura degli elaboratori elettronici a Lui affidati, o comunque sui quali vengano effettuate le sessioni di trattamento dati, ed adoperarsi diligentemente al fine di ridurre al minimo, anche sulla base delle conoscenze acquisite durante gli interventi formativi e comunque in concertazione l'Ente, i rischi che incombono sui dati, ivi compresa la verifica periodica della disponibilità di aggiornamenti del sistema operativo o dei software relativi alla sicurezza dell'elaboratore (a titolo esemplificativo, ma non esaustivo, antivirus, firewall, ecc.).
Gli strumenti elettronici non dovranno essere mai lasciati incustoditi, fatti salvi i casi in cui si sia operata la procedura di log-off.

5) **Modalità per garantire segretezza nelle credenziali elettroniche**: l'incaricato ha l'obbligo di mantenere le proprie credenziali elettroniche segrete, di non diffondere le stesse, di non lasciare scritte e visibili al pubblico dette credenziali, di non comunicarle a colleghi, conoscenti ed amici.

6) **Trasmissione delle modalità accesso al trattamento**: l'incaricato, a fronte della richiesta effettuata dal Responsabile del trattamento o dal Titolare del trattamento, ha il compito di collaborare per la redazione della modalità scritta per l'accesso al trattamento nel caso in cui l'incaricato ne detenga l'accesso esclusivo e sia impossibilitato ad accedere a detto trattamento in tempi brevi. Il documento redatto conterrà anche l'elenco delle persone in possesso delle credenziali elettroniche per accedere al trattamento.

7) **Ambito di trattamento**:l'incaricato può trattare esclusivamente i dati personali che attengono alle funzioni assegnategli e soltanto nell'ambito della tipologia (o delle tipologie) che rientra nei propri incarichi e nel rispetto delle limitazioni dell'ambito di trattamento. Non gli è quindi consentito di eseguire operazioni di trattamento di dati riferiti a soggetti che non rientrino nelle sue competenze o il cui trattamento sia affidato

dal Titolare esclusivamente ad altri soggetti o per fini non previsti tra i propri compiti o dalle disposizioni e regolamenti vigenti nell'Ente.

8) **Cautele nel trattamento dati**: l'incaricato al trattamento ha l'obbligo di adottare tutte le cautele al fine di ridurre i rischi circa la perdita, la distruzione, il danneggiamento dei dati trattati dall'incaricato stesso. L'incaricato ha l'obbligo di ridurre i rischi di accessi non autorizzati ai dati da lui trattati. I trattamenti effettuati dovranno essere svolti nel rispetto della normativa vigente (principio di liceità, finalità, proporzionalità, ecc.) e per perseguire le finalità stabilite dal Titolare.

Custode delle password.

Il custode delle password, laddove eletto, custodirà le credenziali elettroniche degli utenti in busta chiusa, sigillata, riportante il nome dell'incaricato le cui credenziali siano contenute in detta busta, archiviata in apposite casseforti, o mobili equivalenti dotati di chiave di sicurezza, ad accesso esclusivo da parte del custode delle password stesso.
Il custode delle password avrà facoltà di porre in essere, previa richiesta al personale tecnico laddove presente, la procedura di cancellazione delle password degli incaricati, sostituendo le stesse con nuove stringhe di caratteri alfanumerici.
Questa procedura di re-impostazione delle credenziali elettroniche verrà posta in essere laddove:
- vi sia la necessità di accedere ad un trattamento le cui sessioni siano operate in via esclusiva da un incaricato indisponibile per un periodo non compatibile con le finalità del trattamento, gli scopi dell'Ente, i diritti degli interessati;
- non sia possibile creare ulteriori profili di accesso ai dati per incaricati protempore;
- non siano state detenute le password su supporto cartaceo con le modalità sopra indicate e nel rispetto delle modalità indicate nel report "Piani Generali", capitolo Trasmissione modalita' di accesso ai trattamenti dati.

Il custode delle password è indicato per iscritto, laddove eletto.
Il custode delle password avrà il compito di essere a disposizione dell'Ente, degli incaricati del trattamento dati al fine di espletare le sue funzioni nel più breve tempo possibile.
è onere del custode delle password instaurare una procedura e modalità di lavoro, in concerto con i soggetti che sovrintendono la parte di manutenzione degli strumenti elettronici nonché la creazione di apposite impalcature informatiche per nome e conto del Titolare (a titolo esemplificativo software house), tali da non permettergli di leggere in chiaro (cifratura, crittografazione) le password di accesso degli incaricati, e/o dei soggetti operanti sessioni di trattamento in seno alla struttura informatica del Titolare.
Il custode delle password potrà effettuare cambiamenti e cancellazioni delle credenziali elettroniche previo assenso da parte dell'Ente.
Il custode delle password riferirà, oralmente e per iscritto, all'Ente circa la modifica o la cancellazione della componente privata per le credenziali elettroniche (password).

Personale tecnico.
Il Titolare ha facoltà di eleggere il personale tecnico, soggetti che effettuino operazioni di varia natura in seno agli strumenti elettronici adottati per svolgere le sessioni di trattamento o soggetti che svolgano compiti sinergici a tali operazioni e/o equivalenti, al fine di monitorare l'adozione delle misure minime di sicurezza.
Il personale tecnico, oltre all'implementazione delle misure di sicurezza elencate nei punti precedenti, avrà il compito di implementare le seguenti attività:
- predisporre un sistema di autorizzazione informatica con diversi livelli, laddove necessario, di ambito di trattamento;
- impostare gli strumenti elettronici affinchè possano essere gestite, compatibilmente con gli obblighi a carico dei vari soggetti, le credenziali elettroniche di accesso ai trattamenti ed agli strumenti elettronici stessi;
- attribuire un codice identificativo (username, user id) in maniera univoca ed evitando di attribuire lo stesso codice a persone diverse, anche nel corso degli anni;
- aggiornare l'ambito di trattamento ogni qualvolta varino i compiti, le mansioni, l'inquadramento di un soggetto operante sessioni di trattamento per nome e conto dell'Ente ed effettuare la ricognizione del rispetto dell'ambito di trattamento, con cadenza almeno annuale;
- installare programmi volti al limitare il rischio di accesso abusivo agli elaboratori elettronici (615-quinquies del codice penale);
- espletare monitoraggi costanti circa la sicurezza della struttura informatica dell'Ente;
- redigere apposita documentazione riportante i rischi denotati, eventuali azioni da adottare per limitare il livello di rischio.

Il personale tecnico ha il compito di riportare prontamente qualsiasi elemento che possa indurre a ritenere presente e possibile il rischio per la struttura informatica, i dati trattati nonché i diritti degli interessati.

Il personale tecnico è a disposizione dell'Ente al fine di porre in essere tutte le azioni volte a ridurre livelli di rischio o migliorare le modalità di trattamento compatibilmente con la normativa vigente.

allorchè il personale tecnico non sia dipendente dall'Ente, ogni intervento dovrà essere corredato da un rapporto circa le installazioni, manutenzioni effettuate, un rapporto circa quali misure minime di sicurezza siano state ottemperate a fronte dell'intervento eseguito.

Amministratori di sistema, rete, database.
(Fonte Garante Privacy - *Roma, 14 gennaio 2009*)
Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

Per questo il Garante ha deciso di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell' amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo.

Le misure e le cautele dovranno essere messe in atto entro quattro mesi da parte di tutte le aziende private e da tutti i soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia, i servizi di sicurezza. Sono esclusi invece i trattamenti di dati, sia in ambito pubblico che privato, effettuati a fini amministrativo contabile, che pongono minori rischi per gli interessati.

- **Registrazione degli accessi**
  Adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici.
  Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
- **Verifica della attività**
  Verifica almeno annuale da parte dei titolari del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.
- **Elenco degli amministratori di sistema e loro caratteristiche**
  Ciascuna azienda o soggetto pubblico dovrà inserire in un documento interno (disponibile in caso di accertamenti da parte del Garante) gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite.
  Dovranno infine essere valutate con attenzione esperienza, capacità, e affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

24.8 NEW Disposizioni generali in materia di utilizzo dell'Intelligenza Artificiale - AI

È fatto formale divieto agli incaricati al trattamento di utilizzare sistemi di Intelligenza Artificiale per trattare dati personali di cui l'azienda è Titolare, così come trasmettere qualsiasi informazione aziendale a tali sistemi, salvo specifica e formale autorizzazione scritta da parte dell'azienda. Ogni uso non autorizzato sarà considerato una violazione delle policy interne e delle normative vigenti in materia di protezione dei dati personali.

L'uso non autorizzato di Intelligenza Artificiale per trattare dati personali o aziendali comporta rischi significativi per la sicurezza e la riservatezza. Tra i principali rischi vi sono:

1. **Accesso non autorizzato**: Sistemi di AI non controllati o non conformi potrebbero esporre i dati a terze parti, compromettendo la privacy degli interessati e delle informazioni aziendali.
2. **Perdita di controllo sui dati**: L'inserimento di informazioni personali o aziendali in sistemi di AI non approvati può portare alla diffusione o memorizzazione di dati in ambienti non sicuri o al di fuori del controllo aziendale, aumentando il rischio di violazioni e accessi illeciti.
3. **Manipolazione e alterazione dei dati di output:** Algoritmi di AI non verificati potrebbero manipolare o alterare i dati in modo imprevedibile, generando errori o falsificazioni che comprometterebbero l'integrità e l'accuratezza delle informazioni trattate.
4. **Attacchi informatici**: L'uso di AI non autorizzata può rappresentare una vulnerabilità che gli attaccanti informatici potrebbero sfruttare per accedere a sistemi interni, rubare informazioni sensibili o causare danni operativi all'azienda.

Questi rischi sottolineano l'importanza di un utilizzo controllato e autorizzato dell'IA, al fine di proteggere la sicurezza dei dati e di garantire la conformità alle normative in vigore.

24.9 Disposizioni generali in materia di utilizzo delle risorse dell'Ente.

è fatto divieto, salvo espressa autorizzazione (vedasi disciplinari interni eventualmente circolarizzati) scritta da parte del Titolare, Responsabile o persona con poteri equivalenti, di:
- utilizzare degli strumenti elettronici dell'Ente, o di proprietà di terzi ma utilizzati dall'Ente per scopi lavorativi, (p.e. computer, fax, stampanti, ecc.) per finalità non lavorative ovvero per scopi personali;
- installare e/o usare software non espressamente autorizzati dall'Ente;
- operare processi o parte di essi, di file sharing (condivisione di dati e files) o similari, come ad esempio i software di peer to peer, torrent, ecc.;
- salvare files di carattere personale nelle memorie di massa degli elaboratori dell'Ente o utilizzando gli elaboratori dell'Ente;
- utilizzare la casella email attribuita dall'Ente per attività non strettamente correlate alle finalità e/o ai compiti attribuiti dall'Ente all'incaricato al trattamento.

è compito dei soggetti che utilizzano gli strumenti elettronici dell'Ente informare la stessa circa eventi che possano risultare anomali rispetto al consueto iter lavorativo (p.e. apertura di finestre del browser non richieste, possibilità di accesso a dati per i quali non si sia autorizzati o inutili per lo svolgimento dei propri compiti, ecc.).

L'Ente si manleva sin d'ora per qualsiasi violazione, commessa dai soggetti che utilizzano gli strumenti elettronici di proprietà dell'Ente, delle disposizioni illustrate nel presente documento, riservandosi di sanzionare i soggetti inadempienti, salvo che il comportamento degli stessi non costituisca reato allorchè l'Ente si tutelerà nelle opportune maniere e sedi.

Alcuni soggetti sono stati dotati dall'Ente di apposite posizioni di memoria (directory) ove è permesso conservare file personali, sempre nel rispetto delle normative vigenti.
Tale occorrenza è opportunamente indicata nelle lettere di incarico nominali o in equivalenti atti separati.

24.10 Procedure.

A seguire le procedure per un corretto trattamento dei dati.

24.10.1 || 100.100: Ricerca risorse Umane

Attività: Ricerca risorse umane attraverso media diversi e ricezione candidature attraverso Cv
Procedura: La ricerca di risorse umane deve avvenire sempre previa analisi del contesto e dei potenziali interessati ai quale si rivolge la ricerca. In linea generale l'acquisizione di candidature può essere effettuata previa messa a disposizione dell'interessato dell'apposita informativa - anche mediante link alla pagina del sito web aziendale. Tutti i CV debbono essere trattati per la finestra temporale prevista dall'informativa, quindi distrutti. Tutti i CV - se archiviati senza previa lettura fino al momento del loro utilizzo - debbono essere gestiti come contenenti dati estremamente delicati, come ad esempio la disabilità manifestata nel CV e caratterizzante l'interessato.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.2 || 100.110: Assunzione risorsa umana

Attività: Consegna e firma degli atti e documenti susseguenti l'assunzione e formazione della risorsa umana.
Procedura: Tutti i neo assunti hanno l'obbligo di ricevere, e firmare apposita ricevuta, un kit di benvenuto contenente i documenti per effettuare sessioni di trattamenti dati conformi alla vigente normativa ivi compresa il proprio accordo di riservatezza, le istruzioni del titolare in materia di trattamento dei dati, obblighi propri e finalità delle attività di trattamento svolte dai neo assunti, il regolamento interno per l'uso di

strumenti elettronici e generale sulle politiche di tutela dei dati trattati erogate dal titolare al trattamento.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.3 || 100.120: Risorse Umane

Attività: Creazione delle caratteristiche professionali nella risorsa umana per le mansioni ed attività che dovrà svolgere una volta in organico.
Procedura: Tutti i dipendenti debbono essere informati per iscritto circa le modalità di trattamento che il Titolare si aspetta siano seguite dai propri incaricati. In aggiunta, ed a completamento delle istruzioni sopra indicate, le risorse umane dell'azienda debbono seguire corsi di formazione per poter iniziare ad espletare i propri incarichi di lavoro.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.4 || 100.130: Formazione periodica risorse umane

Attività:
Procedura: Tutte le risorse umane dell'Ente e chiunque sia da essa incaricato al trattamento dei dati deve essere oggetto di formazione sistematica nel tempo al fine di poter essere aggiornati su come ridurre ovvero evitare i rischi previsti dalla normativa vigente in materia di trattamento dati, sui nuovi obblighi e modalità di trattamento previste dal titolare, sull'utilizzo consapevole degli strumenti elettronici dati in dotazione dall'Ente.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.5 || 100.140: Informativa e consenso risorse umane

Attività: Gestione Informativa e consenso interessati
Procedura: Le risorse umane appena assunte debbono avere modo di leggere l'informativa al trattamento e prestare il consenso relativo per iscritto. Questo almeno una volta durante il rapporto di lavoro con l'Ente ovvero allorché l'informativa sia variata nella sua sostanza (a titolo esemplificativo ma non esaustivo, modifica delle finalità di trattamento e/o dei mezzi di trattamento).

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.6 || 100.150: Trattamenti senza consenso

Attività: Gestione dei trattamenti dati non legittimati da consenso dell'interessato
Procedura: I trattamenti dati effettuati dall'Ente o da chiunque da essa incaricato, sono effettuabili, previo assenso dell'Ente, se ricorrono le casistiche appresso indicate; in ogni caso è consigliabile rivolgere debito quesito al proprio Consulente Privacy o Data Protection Officer - ove presente. CONTRATTO Trattamento necessario all'esecuzione di un CONTRATTO/misure precontrattuali OBBLIGO LEGALE Trattamento necessario per adempiere un OBBLIGO LEGALE del Titolare del trattamento INTERESSE VITALE Trattamento necessario per la salvaguardia degli INTERESSI VITALI dell'interessato INTERESSE PUBBLICO Trattamento necessario per l'esecuzione di un compito di INTERESSE PUBBLICO o esercizio di pubblici poteri LEGITTIMO INTERESSE Perseguimento del LEGITTIMO INTERESSE del Titolare del trattamento BILANCIAMENTO INTERESSI DIRITTI E LE LIBERTÀ FONDAMENTALI

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.7 || 110.100: Informativa e consenso Clienti

Attività: Gestione Informativa e consenso interessati
Procedura: Tutti i clienti debbono avere a disposizione l'informativa al trattamento ed essere in grado di manifestare il proprio consenso a mezzo atto positivo ed inequivocabile. Il consenso espresso per iscritto si riceve prima dell'inizio dei trattamenti. Il consenso viene richiesto nuovamente laddove ricorrano modifiche significative nella normativa vigente - che ne richiedano la nuova acquisizione anche a fronte di un nuovo modello di informativa - o quando il trattamento sia oggetto di modifica significativa nelle finalità del trattamento e/o nei mezzi utilizzati per effettuare lo stesso.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.8 || 110.120: Notifica dell'esistenza di terzisti per il trattamento dati.

Attività: Laddove l'Ente operi come Responsabile per Titolari terzi al trattamento, è necessario notificare l'esistenza di eventuali sub-Responsabili (dei quali l'Ente si avvale) ad ogni singolo Titolare terzo i cui dati siano trattati da detti sub-Responsabili
Procedura: All'interno del Registro dei Trattamenti per Titolari terzi è stata redatto un testo che riassume i sub-Responsabili dei quali l'Ente si avvale per un dato Titolare terzo. Occorre acquisire detto documento dal proprio responsabile o dall'organo apicale della struttura e

trasmetterlo, previa autorizzazione dai soggetti di cui sopra - al Titolare terzo per il quale si opera. Le attività esternalizzate verso sub-Responsabili possono iniziare solo previa autorizzazione da parte dei Titolari terzi, da acquisirsi per iscritto. Sono equivalenti anche formule contrattuali generiche dove il Titolare terzo autorizzi l'Ente ad avvalersi di sub-Responsabili.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.9 || 120.110: Scelta dei fornitori

Attività: Scelta dei fornitori la cui attività svolta per nome e conto dell'Ente sia costituita, parzialmente o totalmente, dal trattamento dati dei quali l'Ente sia titolare e/o del quale l'Ente sia Responsabile per soggetti terzi
Procedura: La scelta dei fornitori - con particolare riferimento Responsabile verso i quali si esternalizzano attività che comprendono o si basano sul trattamento di dati dei quali l'Ente sia Titolare del trattamento o Responsabile per Titolari terzi - deve avvenire unicamente nei confronti di soggetti che siano in grado di espletare gli incarichi loro affidati nel rispetto della vigente normativa in materia di trattamento dei dati. Le caratteristiche professionali sono testimoniabili dall'esperienza del Responsabile ovvero dall'assenza - nelle fonti di cronaca e/o pagine web disponibili in rete - di reati o inadempienze nei confronti della norma sul trattamento dei dati. La verifica di rispondenza normativa si effettua con la firma del contratto di servizio con l'Ente provvisto dal Consulente Privacy (o altro atto a norma del diritto dell'Unione o dello stato membro) unitamente alla verifica del questionario somministrato al Responsabile. La verifica viene fatta periodicamente ed è funzione - così come eventuali più approfondite modalità di analisi - della delicatezza degli incarichi affidatigli. Le analisi maggiormente approfondite debbono essere riportate per iscritto e disponibili per gli organi di verifica. L'Ente non può affidare incarichi a Responsabili inadatti a svolgere gli stessi ovvero non rispondenti alle prescrizioni della vigente normativa. I Responsabili inadatti o non a norma sono rimossi senza ritardo dalla propria mansione ed i dati loro affidati sono oggetto di retrocessione all'Ente.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.10 || 120.120: Informativa e Consenso - fornitori

Attività: Gestione Informativa e consenso interessati
Procedura: Gestione Informativa e consenso interessati Tutti i fornitori - con particolare riferimento alle ditte individuali, liberi professionisti - debbono avere a disposizione l'informativa al trattamento ed essere in grado di manifestare il proprio consenso a mezzo atto positivo ed inequivocabile. Il consenso espresso per iscritto si riceve prima dell'inizio dei trattamenti. Il consenso viene richiesto nuovamente laddove ricorrano modifiche significative nella normativa vigente - che ne richiedano la nuova acquisizione anche a fronte di un nuovo modello di informativa - o quando il trattamento sia oggetto di modifica significativa nelle finalità del trattamento e/o nei mezzi utilizzati per effettuare lo stesso.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.11 || 130.110: Copia dei dati agli interessati

Attività: Trasmissione di copia dei dati agli interessati a fronte della richiesta degli stessi
Procedura: Affinchè l'interessato eserciti il diritto d'accesso, il Ttitolare al trattamento è tenuto a fornire una copia dei dati oggetto di trattamento a fronte della richiesta dell'interessato. Qualora la richiesta sia presentata dall'interessato in formato elettronico, e salvo sua diversa indicazione, il Titolare trasmette copia dei dati trattati in formato elettronico. A fronte della richiesta dell'interessato di ricevere molteplici copie il Titolare può addebitare all'interessato un contributo spese ragionevole (Art. 15 GDPR).

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.12 || 130.120: Aggiornamento dati interessati

Attività: Aggiornamento dei dati degli interessati a fronte della richiesta degli stessi
Procedura: Nel rispetto del principio di esattezza, il Titolare è tenuto ad aggiornare i dati oggetto di trattamento su richiesta dell'interessato. Allo stesso modo, l'interessato ha diritto di ottenere la rettifica dei dati inesatti e l'integrazione dei dati incompleti, anche fornendo una dichiarazione integrativa (Art. 16 GDPR).

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.13 || 130.130: Cancellazione dati interessati

Attività: Cancellazione dei dati degli interessati a fronte della richiesta degli stessi
Procedura: L'interessato ha diritto di chiedere la cancellazione dei dati oggetto di trattamento ed il Titolare procede alla cancellazione senza ingiustificato quando: - non sussistono più le finalità del trattamento; - l'interessato ho revocato il consenso sul quale si basava il trattamento; - l'interessato si oppone ai trattamenti ai sensi dell'art. 21 GDPR; - i dati sono oggetto di trattamento illecito; - la cancellazione costituisce obbligo legale per il titolare; - i dati sono stati raccolti in relazione all'offerta di servizi della società dell'informazione. (Art. 17 GDPR).

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.14 || 130.140: Limitazione al trattamento dei dati

Attività: Limitazione dei dati trattati degli interessati a fronte della richiesta degli stessi.
Procedura: L'interessato ha diritto ad ottenere la limitazione del trattamento dei dati da parte del Titolare: - nel periodo in cui il Titolare verifica l'esattezza dei dati su richiesta dell'interessato; - quando i dati sono oggetto di trattamento illecito e l'interessato si oppone alla cancellazione; - quando, sebbene il Titolare non ne abbia più bisogno, l'interessato necessita dei dati in sede giurisdizionale; - nel periodo in cui il Titolare verifica l'esistenza di motivi legittimi prevalenti a fronte della opposizione al trattamento effettuata dall'interessato. (Art. 18).

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.15 || 130.150: Notifica incombente sblocco limitazione trattamento dati

Attività: Il Titolare al trattamento, anche attraverso attività svolte dal Responsabile, deve informare l'interessato circa l'avvenuta rettifica, cancellazione, limitazione del trattamento, a fronte delle richieste dell'interessato. Stesso obbligo di notifica va seguito prima dello sblocco della limitazione del trattamento che può avvenire automaticamente dopo qualche tempo dalla richiesta dell'interessato.
Procedura: Prima di dare corso allo sblocco della limitazione del trattamento, occorre informare l'interessato il quale potrebbe rinnovare la richiesta di limitazione. Occorre indicare una data entro la quale lo sblocco avverrà e dare una data entro la quale l'interessato potrà rinnovare la propria richiesta. In caso di silenzio si potrà procedere con lo sblocco del trattamento. Occorre dare non meno di una settimana (meglio 14 gg) all'interessato per poter esprimere la propria volontà in merito allo sblocco della limitazione di trattamento. La trasmissione dell'informazione deve avvenire attraverso i mezzi di contatto indicati dall'interessato. Sarebbe auspicabile inviare una pec, in subordine una email, in subordine un fax, in subordine telefonare all'interessato. Tenere traccia di questa situazione all'interno del fascicolo dell'interessato.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.16 || 130.160: Notifica avvenuta rettifica, cancellazione, limitazione trattamento dati

Attività: Il Titolare al trattamento, anche attraverso attività svolte dal Responsabile, deve informare l'interessato circa l'avvenuta rettifica, cancellazione, limitazione del trattamento, a fronte delle richieste dell'interessato. Stesso obbligo di notifica va seguito prima dello sblocco della limitazione del trattamento che può avvenire automaticamente dopo qualche tempo dalla richiesta dell'interessato.
Procedura: Al momento in cui si da corso alla richiesta dell'interessato (opportunamente identificato) circa la rettifica, cancellazione, limitazione del trattamento, occorre informare l'interessato. La trasmissione dell'informazione deve avvenire attraverso i mezzi di contatto indicati dall'interessato. Sarebbe auspicabile inviare una pec, in subordine una email, in subordine un fax, in subordine telefonare all'interessato. Tenere traccia di questa situazione all'interno del fascicolo dell'interessato.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.17 || 140.110: Comunicazione dati contatto data protection all'autorità Garante

Attività: Comunicazione dati contatto DPO ad autorità Garante attraverso procedure identificate da autorità stessa.
Procedura: I dati di contatto del DPO sono comunicati non appena possibile all'Autorità Garante per la privacy, a mezzo email, utilizzando il modello disponibile su http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322292 In subordine il modello può essere richiesto al DPO stesso. I dati di contatto via email, del DPO, sono presenti nelle informative al trattamento dell'Ente, sul sito web del Titolare al trattamento. I dati del DPO sono aggiornati allorché lo stesso sia sostituito da altro soggetto.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.18 || 140.115: Creazione dati contatto data protection

Attività: Messa a disposizione degli interessati dei dati di contatto del Titolare al trattamento (caselle email, indirizzi, numeri di telefono ivi compresi i dati del DPO ove presente)
Procedura: I dati di contatto (casella email e, se del caso, telefoni, indirizzi, etc.) del referente presso la struttura del Titolare, dei Responsabili - se necessario, del Rappresentante sul territorio comunitario, del Data Protection Officer - se eletto, sono resi disponibili per gli interessati attraverso pubblicazione sul sito internet della società.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.19 || 140.120: Adozione del DPIA

Attività: Il DPIA viene adottato ogni qualvolta : - il trattamento comporti un rischio alto (massima gravità per massima possibilità di accadimento) possa presentare un rischio elevato per le libertà ed i diritti delle persone fisiche; - il trattamento comporti una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; - il trattamento

utilizzi, su larga scala, categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico; - il trattamento sia inserito nell'elenco dei trattamenti per i quali sia obbligatorio il DPIA e pubblicato dall'Autorità Garante.
Procedura: La redazione del DPIA è effettuata attraverso professionista o dipendente dell'Ente prima dell'inizio delle sessioni di trattamento e deve essere terminato prima dell'inizio delle stesse. Laddove le misure previste nel DPIA non indichino come calmierati ed accettabili i rischi relativi alle dignità ed alle liberta degli interessati, sarà necessario richiedere preventiva autorizzazione all'Autorità Garante attraverso apposito interpello. Il Titolare al trattamento consulta il DPO ove presente circa la necessità e l'adozione del DPIA.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.20 || 140.130: Gestione del DPIA

Attività: Gestione del piano di impatto sulla protezione dei dati.
Procedura: Successivamente e periodicamente all'implementazione del DPIA, i trattamenti che l'hanno originato sono oggetto di valutazione per verificare che gli stessi siano effettuati conformemente alla valutazione d'impatto. Ogni volta che insorgano variazioni dei rischi afferenti alle attività di trattamento e contenute nel DPIA - siano esse derivanti dalla variazione del contesto o dei dati trattati - il DPIA è oggetto di riesame.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.21 || 140.140: Gestione dei Data Breach - notifica all'Autorità Garante

Attività: Gestione della notifica all'Autorità Garante relativa agli accessi illeciti ai dati personali trattati dall'Ente
Procedura: Laddove vi sia un Data Breach - sia esso per volontà come, per esempio, la violazione da parte di un soggetto terzo nei confronti del domicilio informatico ed il conseguente accesso ai dati in esso contenuti, sia esso derivante dalla presa di possesso di supporti (documentali o informatici) che contengono dati personali, a causa di perdita (la perdita di una chiavetta usb) o di furto - lo stesso deve essere notificato senza ingiustificato ritardo - ovvero entro 72 ore massimo dal momento in cui si viene a conoscenza del Data Breach - all'Autorità Garante. Laddove la notificazione sia effettuata oltre le 72 ore dalla presa di coscienza del Data Breach, la stessa è corredata dalle motivazioni che hanno causato il ritardo. Laddove si operi come Responsabile del trattamento ed in caso di Data Breach, si provvede ad informare il Titolare / i Titolari del trattamento senza ingiustificato ritardo. Il modulo da utilizzare è reperibile su http://www.garanteprivacy.it/home/modulistica alla voce Data Breach.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.22 || 140.150: Gestione dei Data Breach - notifica interessati

Attività: Gestione della notifica agli interessati relativa agli accessi illeciti ai dati personali trattati dall'Ente
Procedura: In caso di Data Breach si procede senza ingiustificato ritardo alla comunicazione dell'avvenuta violazione nei confronti di tutti gli interessati dalla violazione stessa. La natura e conseguenze della violazione sono descritte con un lessico semplice e chiaro. La comunicazione contiene i dati di contatto del DPO, ove eletto, le conseguenze per la persona fisica derivanti dalla violazione, le misure adottate o che saranno adottate per porre rimedio alle conseguenze ovvero attenuare gli effetti negativi delle stesse. La comunicazione non è effettuata se ricorrono i seguenti motivi: - i dati non oggetto di Data Breach sono trattati tecnicamente in modo da renderli non leggibili se non in possesso delle apposite credenziali (p.e. cifratura); - successivamente al Data Breach il Titolare ha adottato le misure tecniche necessarie per scongiurare il sopraggiungere di rischi elevati sulle libertà e le dignità degli interessati; - la comunicazione richiede sforzi sproporzionati, in tal caso si procede con una comunicazione pubblica. La violazione potrebbe essere oggetto di obbligo di comunicazione stante la valutazione dell'Autorità Garante.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.23 || 140.160: Redazione delle policy

Attività: Redazione ed aggiornamento dei regolamenti aziendali in materia di trattamento dati nonché utilizzo degli strumenti elettronici.
Procedura: Le policy in materia di tutela dei dati personali sono prodotte dal Titolare al trattamento per i propri incaricati e sono nuovamente circolarizzate ogni qualvolta sia apportata una modifica alle stesse. Le policy sono oggetto di aggiornamento in occasione di modifiche normative, significative modifiche degli strumenti elettronici utilizzati, significative modifiche dei trattamenti effettuati. Le policy sono modificate dal consulente al trattamento, se presente, o dal personale interno all'azienda previo assenso del Titolare o di persona da lui preposta.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.24 || 140.170: Audit Annuali data protection

Attività: Gestione degli audit periodici - main audit e sorveglianze successive - finalizzati a verificare la rispondenza dell'Ente nei confronti della vigente normativa in materia di trattamento dati.
Procedura: Con cadenza almeno annuale sono effettuati audit finalizzati a: - mappatura dei trattamenti, delle aggregazioni concettuali di dati, delle classi di dati - verifica dei dati trattati - analisi e mappatura dei rischi - analisi misure adottate e modifiche da apportare sulle stesse - verifica dell'adeguatezza dei ruoli affidati in azienda con particolare riferimento verso i Responsabili - verifica del livello di formazione delle risorse umane incaricate al trattamento - verifica ed aggiornamento del Registro dei trattamenti - verifica della presenza dei necessari DPIA nonché loro efficacia

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.25 || 140.180: Verifica di implementazione delle misure prescritte

Attività: Verifica di corretta applicazione delle misure stabilite per rendere l'Ente rispondente alla vigente normativa in materia di trattamento dati.
Procedura: Con cadenza periodica i responsabili delle varie aree verificano che le misure previste per la propria attività, siano implementate e correttamente applicate. Il DPO - laddove eletto, o il Consulente Privacy o soggetto equivalente, verificano periodicamente le misure attraverso audit periodici con cadenza almeno annuale.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.26 || 140.190: Verifica attribuzione ruoli all'interno dell'Ente

Attività: Verifica dell'attribuzione dei ruoli ai dipendenti operanti sessioni di trattamento per nome e conto dell'Ente.
Procedura: Qualsiasi ruolo affidato dall'Ente e rientrante nel GDPR può essere affidato a soggetti che sono adatti a ricoprire l'incarico, sono informati e formati preventivamente all'inizio delle sessioni di trattamento, formati periodicamente in occasione di modifiche tecniche, tecnologiche, logistiche, procedurali, normative relativamente alle proprie mansioni. La valutazione di adeguatezza del soggetto dovrebbe essere effettuata a fronte dell'acquisizione della sua Job Description (descrizione testuale delle attività che il soggetto svolgerà per nome e conto dell'Ente). L'attività di valutazione è maggiormente importante per quanto attiene i Responsabili (siano essi insourcing che outsourcing) poiché su essi grava anche l'onere di essere rispondenti alla vigente normativa - in difetto di rispondenza il Responsabile diventa automaticamente Titolare con le conseguenze legali del caso - mentre sul Titolare grava l'onere di controllo. I livelli di controllo potranno essere tre: - controllo di primo livello, dove l'Ente emette una lettera di incarico, contratto per il trattamento dei dati, accordo di riservatezza, etc., contenente - tra le altre cose - le istruzioni operative, compiti responsabilità, obblighi, modalità e mezzi di trattamento; - controllo di secondo livello, dove l'Ente trasmette un questionario specifico al soggetto, relativo alle attività da lui svolte; - controllo di terzo livello, dove l'Ente invia un soggetto - sia esso il DPO, il Consulente Privacy o soggetto equivalente - presso la struttura del Responsabile ovvero presso l'incaricato che tratta i dati; l'incontro è finalizzato alla verifica di rispondenza normativa ovvero di capacità di assolvere l'incarico affidato nel rispetto delle vigenti norme in materia. I soggetti che non sono stati verificati o che non sono in grado (per carenze personali o della propria struttura, sia in termini professionali che in termini di rispondenza normativa) non possono trattare i dati; in caso di professionisti l'incarico dovrebbe essere interrotto dall'Ente fino al raggiungimento del livello necessario per operare le sessioni di trattamento. In caso di interruzione del rapporto con un Responsabile gli organi apicali della struttura, il DPO - ove eletto, il Consulente Privacy o soggetto equivalente, sono informati per iscritto al fine di effettuare una valutazione più funzionale per la data protection e relativa al soggetto.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.27 || 140.200: Data Breach in qualità di Responsabile operante per Titolari terzi

Attività: Laddove l'Ente operi in qualità di Responsabile per Titolari terzi e laddove l'Ente riscontri l'avvenuto Data Breach, è necessario informare i Titolari terzi i cui dati sono stati coinvolti nel Data Breach.
Procedura: Il Data Breach per i dati trattati per nome e conto di Titolari terzi segue le regole e modalità di verifica e reazione per i Data Breach avvenuti su dati di cui si sia Titolari. Il Titolare terzo è informato senza ingiustificato ritardo circa: - natura e violazione dei dati personali, - categorie e numero approssimativo degli interessati; - numero approssimativo delle registrazioni di dati coinvolte (numero di record nel caso di database); - dati di contatto del DPO se presente, o del Consulente Privacy o soggetto equivalente; - conseguenze potenziali; - misure adottate o che verranno adottate per porre rimedio ovvero attenuare gli effetti negativi. Laddove non sia possibile trasferire queste informazioni immediatamente, le si trasferirà senza ingiustificato ritardo appena possibile. Il Data Breach deve essere inserito nel Registro delle violazioni che ogni soggetto deve tenere, quindi comunicato agli organi apicali della struttura, al soggetto detenente la responsabilità IT o altro soggetto preposto, al fine di mantenere traccia centralizzate degli eventi dannosi occorsi sui dati. Il DPO riceve copia del Registro degli eventi dannosi aggiornato.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.28 || 150.100: Tutela contro accessi abusivi agli strumenti elettronici

Attività: Attività strumentali per ridurre i rischi di accesso abusivo agli strumenti elettronici (hardware e software) attraverso i quali sono trattati i dati da parte dell'Ente
Procedura: Il soggetto detenente la responsabilità IT redige le modalità di tutela per limitare il verificarsi di accessi abusivi agli strumenti

elettronici (hw e sw) - con particolare riferimento ai dati personali in essi contenuti - sia da parte dell'insieme di soggetti esterno all'Ente, che da parte dall'insieme dei soggetti che a vario titolo sono all'interno della struttura dell'Ente (intesa come struttura informatica o logsitica). La procedura contiene le misure tecniche ed organizzative atte a ridurre adeguatamente il rischio ad un livello accettabile; più specificamente si dovranno ridurre i rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso accidentale o illegale ai dati personali trattati dall'Ente. Le misure possono includere tecniche di pseudonimizzazione e cifratura. Le misure debbono essere mirate anche alla capacità di assicurare su base permanente: - la Riservatezza Integrità e Disponibilità (laddove i coefficienti RID sono stati espressi dal management, nell'atto di modulare le misure, si tenga in debita considerazione i livello basso, medio, alto richiesto dal management relativamente alla Riservatezza Integrità e Disponibilità dei dati); - la resilienza dei sistemi e servizi di trattamento; - la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali (anche in caso di incidente tecnico o fisico degli strumenti elettronici o delle aree logistiche in esse contenuti); - nell'ottica di un ciclo PLAN-DO-CHECK-ACT, una procedura per testare, verificare, valutare, migliorare regolarmente l'efficacia delle misure adottate. Le misure sono preventivamente discusse con il DPO - ove presente - o con il soggetto che gestisce la Data Protection (Consulente Privacy o equivalente). All'atto dell'avvenuta implementazione, dette misure, sono comunicate al soggetto di cui sopra per implementazione negli atti redatti (Registro dei trattamenti, Piano di Impatto sulla protezione dei dati, etc.) nonché per ulteriore valutazione circa la loro efficacia. La verifica di efficacia è effettuata con cadenza periodica stabilita preventivamente l'implementazione delle misure.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.29 || 150.110: Gestione accessi abusivi avvenuti

Attività: Gestione degli accessi abusivi avvenuti
Procedura: Laddove, attraverso le misure implementate nella struttura dell'Ente o attraverso altre modalità, si verifichi che vi sia stato un accesso abusivo ai dati trattati, il soggetto detenente la responsabilità IT deve, senza ingiustificato ritardo ovvero immediatamente al momento della presa di coscienza dell'avvenuto accesso abusivo, informare i propri responsabili ovvero gli organi apicali dell'Ente. Laddove presente il DPO - o il Consulente Privacy o soggetto equivalente - viene informato con le stesse modalità. L'informazione avviene attraverso comunicazioni scritte (anche via email), circostanziate e con l'uso di lessico accessibile anche ai soggetti non tecnici con conseguente telefonata per verificare che la comunicazione sia stata ricevuta. Immediatamente si pongono in essere le attività per interrompere l'accesso abusivo ovvero ridurre al minimo le conseguenze, nei confronti degli interessati, dell'evento dannoso. Una volta attuate le contromisure in reazione all'evento, il soggetto detenente la responsabilità IT si incontra con gli organi apicali dell'Ente - o soggetto da loro indicato, con il DPO - o con il Consulente Privacy o soggetto equivalente, al fine di stabilire le misure ulteriori. Dette ulteriori misure sono finalizzate a limitare ulteriormente le conseguenze del verificarsi del rischio ovvero limitare eventi similari in futuro.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.30 || 150.1101: Gestione accessi abusivi avvenuti

Attività: Gestione degli accessi abusivi avvenuti
Procedura: Qualsiasi accesso abusivo ai dati personali e/o agli strumenti elettronici che permettono l'accesso a detti dati (quali a titolo esemplificativo, ma non esaustivo, hardware o software, computer, hard disk, memorie di massa diverse quali usb memory stick e similari, smart phone, palmari, tablet, etc.) è: - riportato per iscritto nel Registro degli eventi dannosi occorsi (un file che ogni utente può tenere per proprio conto ma che deve essere comunicato al soggetto detenente la responsabilità IT); - l'evento dannoso riportato nel Registro contiene informazioni sulla data di scoperta dell'evento, la data presunta di primo accesso abusivo ai dati, quali dati personali, servizi, hardware, software sono stati veicolo dell'accesso abusivo, quali le motivazioni che hanno portato all'evento, quali i soggetti presumibilmente hanno causato con il proprio comportamento il verificarsi dell'evento; - l'evento dannoso è comunicato al DPO, se presente, oppure - in subordine - al Consulente Privacy o soggetto equivalente; - la comunicazione, registrazione evento nel Registro, sono effettuate per iscritto.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.31 || 150.120: Analisi dei rischi IT

Attività: Redazione dell'analisi dei rischi relativamente ai dati trattati attraverso gli strumenti elettronici (hardware e software) di propria competenza.
Procedura: Il soggetto detenente la responsabilità IT effettua analisi dei rischi incombenti sui dati valutando gli strumenti elettronici hw e sw, i servizi erogati agli incaricati nonché i servizi automatizzati, con particolare riferimento ai rischi derivanti da perdita, distruzione, modifica, divulgazione non autorizzata, accesso accidentale per soggetti non autorizzati o illegale, relativamente ai dati personali. I livelli di Riservatezza, Integrità e Disponibilità (RID), stabiliti dall'Ente direttamente attraverso i propri organi apicali ovvero attraverso media delle valutazioni espresse dai responsabili dei vari processi aziendali, sono altresì da tenersi in debita considerazione per la modulazione delle misure derivanti dall'analisi e valutazione dei rischi

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.32 || 150.130: Implementazione di nuovi strumenti elettronici

Attività: Processo di gestione dell'implementazione, ivi compresa la fase progettuale, di nuovi strumenti elettronici (hardware e software)
Procedura: Qualsiasi strumento elettronico utilizzato per trattare dati o accedere ulteriormente a strumenti elettronici preposti al trattamento di dati personali, prima della sua implementazione deve essere validato dal soggetto detenente la responsabilità IT che effettua un'analisi dei rischi su detto strumento.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.33 || 150.140: Utilizzo strumenti elettronici SW a norma.

Attività: L'Ente ha l'obbligo di utilizzare strumenti elettronici rispondenti alle prescrizioni della vigente normativa (privacy by design, privacy by default)
Procedura: Ogni strumento il cui utilizzo è previsto, che viene acquistato, implementato o fruito all'interno della struttura dell'Ente e che è utilizzato per trattare dati personali, deve rispondere alla vigente normativa con particolare riferimento alla definizione privacy by design (il software deve essere stato ingegnerizzanto prevedendo di rispettare le prescrizioni per la data protection unitamente alla limitazione dei rischi previsti dalle norme in materia) nonché alla definizione di privacy by default (le impostazioni predefinite dovranno essere mirate a tutelare i diritti degli interessati nonché rispondere alla vigente normativa anche relativa a questi aspetti). Per ottemperare a queste prescrizioni è necessario ottenere la garanzia da parte del produttore (che dovrà avere riscontro poi nella realtà e durante l'utilizzo del software) che dichiari la conformità del software, in maniera netta ed inequivocabile. I software certificati privacy a norma del GDPR possono essere considerati come rispondenti alla vigente normativa: verificare per quale tipo di attività, processo o trattamento il software è stato certificato poiché si potrebbero avere certificazioni di rispondenza normativa anche di parte del funzionamento del software.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.34 || 160.100: Nuovi processi di trattamento

Attività: Gestione dei trattamenti dati derivanti da nuovi processi che la Governance desideri realizzare
Procedura: Qualora il Titolare al trattamento implementi o modifichi i processi e le attività da esso svolte con conseguente mutamento nel trattamento dei dati, è tenuto a raccogliere un nuovo consenso presso gli interessati i cui dati sono riferiti.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.35 || 190.100: Preparazione sistema

Attività: Attività preliminari di preparazione ed impianto del sistema di whistleblowing, concernenti la progettazione del trattamento, la scelta dei soggetti coinvolti, la redazione dei documenti.
Procedura: La Governance e la funzione legale preposta, di concerto con il Dpo, progetta il trattamento in tutte le sue fasi. Il Dpo assicura che il trattamento sia conforme alle normative vigenti per quanto attiene la data protection, nonché' valuta misure idonee per tutelare i diritti degli interessati. Questa attività include: - l'analisi dei rischi sui dati trattati; - la valutazione di impatto (Dpia) sul trattamento ed eventuale software; - la redazione dei contratti di trattamento (per responsabili ed amministratori di sistema laddove vi sia utilizzato un software come canale di comunicazione o attività similari); - la redazione di istruzioni operative ed accordi di riservatezza per personale interno alla struttura dell'ente; - la redazione delle idonee policy in materia di trattamento dati derivante dall'adozione della disciplina del whistleblowing. Solo dopo l'effettuazione ed il superamento delle attività di data protection, il trattamento potrà iniziare.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.36 || 190.110: Prima ricezione e valutazione segnalazione

Attività: Attività di ricezione della segnalazione, valutazione di pertinenza per il d.lgs. 24/2023, verifica dell'identità del segnalante, valutazione di esistenza del reato, trasmissione alla funzione aziendale preposta
Procedura: Il Gestore della segnalazione riceve i dati sulla segnalazione e sull'identità del segnalante. Detti dati sono connotati dai seguenti livelli di r.i.d., salvo diversa indicazione da parte dell'ente. - riservatezza: dati ad alta riservatezza - integrità: dati ad alta garanzia di integrità - disponibilità: dati ad alta garanzia di disponibilità Nel valutare l'identità del Segnalante e la segnalazione, il Gestore adotta tutte le misure idonee affinché' i parametri r.i.d. di cui sopra siano garantiti. Laddove questo non sia possibile, il Gestore richiede intervento del Dpo. Laddove la segnalazione arrivi attraverso documento scritto, il Gestore assicura che l'identità del Segnalante sia contenuta in busta chiusa e la segnalazione in differente busta chiusa e che entrambe siano indirizzate a cassetta di posta ove il Gestore abbia accesso esclusivo. Il Gestore archivia detti documenti in archivio cartaceo ad accesso esclusivo, dotato di serratura, la cui chiave sia in possesso unicamente del Gestore. Il Gestore adotta misure atte a verificare immediatamente eventuali violazioni di riservatezza dei documenti. Laddove la segnalazione avvenga attraverso file audio contenente la voce del segnalante, il Gestore assicura la riservatezza del file salvando lo stesso all'interno di una memoria di massa rimuovibile (p.e. usb conservata in mobilia ad accesso esclusivo del Gestore) o in una directory di proprio esclusivo accesso in computer dotato degli strumenti elettronici previsti dall'ente per la sicurezza it. In entrambi i casi il Gestore si confronta preliminarmente con il Dpo circa le attività scelte: il Dpo emette parere preliminare all'uopo. Laddove la segnalazione avvenga attraverso software scelto dall'ente, il Gestore si attiene alle misure già previste in fase di progettazione dal Dpo di concerto con la funzione legale e la governance. La gestione del rapporto con il Segnalante e gli approfondimenti necessari ovvero i resoconti delle attività svolte susseguenti la segnalazione, sono effettuate in ambienti riservati ed al riparo da terzi non autorizzati al trattamento di detti dati. Il Gestore garantisce la riservatezza di questi dati,

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.37 || 190.120: Gestione della segnalazione

Attività: Attività di gestione della segnalazione, gestione dei dati su strumenti elettronici, trasmissione - in parte o in toto - in chiaro a terzi necessari per l'adozione delle misure idonee.
Procedura: La gestione della segnalazione, intendendo con questo termine la trasmissione alla funzione competente per l'attività di mitigazione del reato (destinatario della segnalazione), avviene in considerazione del fatto che dati della segnalazione potrebbero permettere: • l'identificazione del Segnalante e/o sono collegati allo stesso attraverso l'id della segnalazione; • l'identificazione dei Facilitatori e dei Colleghi del Segnalante; • l'identificazione dei soggetti Segnalati. A fronte di quanto sopra: • i dati della segnalazione, riferibili al segnalante, sono da considerarsi pseudonimizzati. Detti dati debbono, di conseguenza, essere trattati come dati personali, comprendendo le cautele del caso; • i dati della segnalazione, riferiti a terzi eventualmente coinvolti dall'evento, sono da considerarsi dati personali a tutti gli effetti (con possibilità di trattamento di dati particolari/sensibili e giudiziari). Il Gestore, prima di procedere con la trasmissione della segnalazione alla funzione aziendale destinataria, si confronta con il Dpo per la valutazione del singolo caso. Il Gestore indica quale funzione aziendale sarà destinataria della comunicazione. Il Dpo provvede alla redazione di apposito accordo di riservatezza/istruzioni operative (per i dipendenti) ovvero contratto di trattamento (per responsabili al trattamento). Il documento ha la finalità, tra le altre, di sensibilizzare il destinatario della segnalazione affinché' mantenga il più stretto riserbo sui dati contenuti nella segnalazione, al fine di assicurare un alto livello di riservatezza sull'identità del Segnalante ovvero si renda il piu' remoto possibile ricongiungere i dati della segnalazione ad una persona fisica. Solo dopo l'avvenuta firma di detti documenti si potrà procedere con la trasmissione della segnalazione. Qualsiasi destinatario della segnalazione può trasmettere i dati a terzi solo se detti soggetti sono istruiti in tal senso dal Titolare al trattamento ed hanno ricevuto e sottoscritto idonea lettera di incarico (accordo riservatezza / istruzioni operative).

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.10.38 || 190.130: Chiusura della segnalazione e cancellazione dei dati

Attività: Attività di chiusura della segnalazione, sia per mancanza di evidenze che la rendano rientrante nel d.lgs. 24/2023 sia per termine delle attività, cancellazione dei dati immediata o posticipata a seconda che la segnalazione sia risultata pertinente o meno.
Procedura: Laddove la segnalazione non sia ritenuta idonea poiché' non rientrante nella disciplina del Whistleblowing, si procederà alla cancellazione dei dati di concerto con il Dpo. Laddove la segnalazione sia ritenuta rientrante nella disciplina del Whistleblowing, si effettuerà la cancellazione trascorsi cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, o fino alla conclusione del procedimento giudiziale o disciplinare eventualmente conseguito nei confronti del Segnalato o del Segnalante. Il Gestore della segnalazione indica la data di cancellazione dei record collegati alla segnalazione, notificandola al Titolare del trattamento, nel rispetto delle tempistiche sopra indicate. Debita procedura informatica automatizzata di cancellazione è impostata all'interno della Piattaforma informatica per la gestione del Whistleblowing. Laddove la procedura automatizzata non sia possibile il Gestore della segnalazione segnala la necessità di cancellazione dei record, una settimana prima della data di cancellazione dei dati, al Titolare del trattamento e, appena ricevuto assenso, provvede alla cancellazione manuale dei file affinché detti file non siano tecnicamente più ricostruibili.

Tutte le figure professionali presenti nell'Ente debbono seguire la presente procedura, durante l'espletamento dell'attività sopra descritta.

24.11 MISURE PREVISTE DA NORME & BEST PRACTICE.

A seguire l'elenco deii requisiti di sicurezza obbligatori per legge e previsti nel Testo Unico in Materia di Dati Personali. Tali misure sono relative unicamente ai trattamenti posti in essere nell'Ente nonché alla tipologia di dati trattati.

Si informa, infine, che, ai sensi dell'art.29 del Codice, il Titolare del trattamento disporrà di verifiche e controlli periodici circa la puntuale osservanza delle disposizioni di cui al presente regolamento.

Politiche di riutilizzo delle memorie di massa.

Misure di sicurezza da adottarsi per lo smaltimento o il reimpiego di rifiuti di apparecchiature elettriche ed elettroniche.

In data 13 ottobre 2008, con pubblicazione sulla G.U. n° 287, in data 9 dicembre 2008, è stata data diffusione alle misure di sicurezza previste per evitare la persistenza di dati personali, sensibili, giudiziari, su supporti di memorizzazione allorché gli stessi siano oggetto di smaltimento o reimpiego.
Non tutti sanno che i dati contenuti in molti strumenti elettronici con capacità di memorizzazione - primi tra tutti gli elaboratori - effettuano la cancellazione dei file eliminando la loro esistenza da una sorta di mappatura interna (detta FAT - File Allocation Table o NTFS - New Technology File System) ovvero tavola di allocazione dei file. Il file cancellato dalla mappatura generale è ricostruibile e utilizzabile, a mezzo di appositi programmi che ne identificano l'esatta collocazione all'interno del supporto, fino a quando le parti dello stesso non sono state sovrascritte (in toto o in parte) da altri dati. Tali sistemi sono ben noti, per esempio, alla Guardia di Finanza e sono in grado di ricostruire i dati cancellati (per esempio relativi ad eventuali evasioni fiscali), trattati sull'elaboratore dell'azienda oggetto di verifica. Vi sono programmi finalizzati alla distruzione definitiva dei file prodotti attraverso la riscrittura, con caratteri casuali, dei settori che ospitavano le parti dei file cancellati.

Ambito di applicazione.
Le presenti misure riguardano le operazioni di distruzione, dismissione, reimpiego, di supporti contenenti dati personali, sensibili, giudiziari, con particolare riferimento a PC, palmari, telefonini, memorie di massa (hard disk, dvd, chiavette usb, etc.), utilizzate da soggetti pubblici o privati con particolare riferimento ad attività commerciali, industriali, professionali, istituzionali.

Soggetti operanti la distruzione dei dati.
Le operazioni di distruzione dei dati possono essere affidate a dipendenti dell'azienda, operanti sotto le direttive del titolare del trattamento, o soggetti esterni. Nel caso in cui si decida di affidare a soggetti esterni dette attività, occorre ricercare aziende tecnicamente qualificate e che attestino l'avvenuta gestione dei supporti di memorizzazione, secondo la vigente normativa. Il testo unico in materia di trattamento dati richiama, a tal scopo, l'attenzione del titolare al trattamento circa l'obbligo di ricevere attestazioni di conformità laddove le misure di sicurezza siano state adottate servendosi di soggetti esterni: questa procedura si concretizza con la ricezione del "rapporto degli installatori esterni" ovvero apposito documento ove l'azienda, fornitore del servizio, attesta di aver eseguito correttamente l'attività affidatale, manlevando il titolare al trattamento da qualsivoglia inadempienza derivante da detto incarico.
Coloro che reimpiegano o riciclano i supporti di memorizzazione hanno l'obbligo di verificare l'inesistenza dei dati e, in caso di verifica negativa, informare prontamente il titolare, richiedere autorizzazione alla distruzione dei dati, cancellare gli stessi verificando la non intelligibilità dei dati.

Modalità di reimpiego RAEE.
Al fine di rendere non tecnicamente ricostruibili i dati, vi sono misure di natura preventiva che il titolare può adottare. La creazione di file, o collezione di file, cifrate a mezzo di password può essere agevole laddove si tratti di operazioni da espletare non sistematicamente. Per i soggetti che trattano sistematicamente dati personali, o sensibili o giudiziari, hanno bisogno di sistemi meno invasivi. I più moderni sistemi operativi (p.e. Windows XP Pro) permettono la cifratura di interi hard disk (o memorie di massa similari) senza richiedere la password di cifratura ogni volta: il sistema operativo cifra e decifra i file non appena sono salvati / letti, utilizzando una chiave di cifratura creata – dal sistema operativo – al momento della creazione dell'account dell'incaricato al trattamento. I dati rimarranno leggibili anche dopo il cambiamento periodico della password. In caso di azzeramento del sistema operativo (p.e. reinstallazione dello stesso) i dati potrebbero non essere più recuperabili se non previo reinserimento chiave di crittografazione create dal precedente sistema operativo installato.
Oltre alle misure preventive, debbono essere adottate misure apposite prima del reimpiego dei supporti.
Tali misure si concretizzano nella:

- cancellazione e sovrascrittura con caratteri casuali dei file, ripetendo l'operazione da sette a trentacinque volte; tale operazione può protrarsi da alcuni minuti a diversi giorni;
- formattazione di basso livello (low level formatting), con conseguenti rischi per l'integrità del supporto;
- demagnetizzazione del supporto, relativa unicamente ai supporti magnetici quali hard disk, dischi magneto-ottici, floppy disk, cassette DAT, etc. ma inefficacie su supporti quali cd, dvd, etc.; tale attività rende necessario l'accesso fisico alla memoria di massa che risulta essere non sempre agevole.

Modalità di smaltimento RAEE.
Obiettivo dello smaltimento sicuro è, come per il reimpiego, la distruzione dei dati. A differenza del reimpiego dei supporti, in caso di distruzione è percorribile la strada che porta al danneggiamento del supporto che ospita i dati.
Nello specifico, oltre le tecniche descritte per il reimpiego dei supporti, è possibile utilizzare:

- sistemi di punzonatura;
- sistemi di deformazione meccanica;
- distruzione fisica o disintegrazione, particolarmente utilizzati per supporti quali CD e DVD;

demagnetizzazione ad alta densità con conseguente danneggiamento anche dei microchip costituenti la struttura di servizio del supporto (basti pensare agli hard disk).

24.11.1 Modalità per trattamenti di dati senza l'ausilio di strumenti elettronici

I dati - anche su supporto cartaceo - sono sempre sotto la responsabilità del soggetto che li tratta (anche se su autorizzazione del titolare del trattamento),
il quale ne deve curare la diligente custodia nonché
minimizzare i rischi di violazione di
Riservatezza, Integrità e Disponibilità degli stessi.

I dati possono essere trattati nell'Ente senza l'ausilio di strumenti elettronici se sono ottemperate le seguenti misure.

Periodicamente (suggerito con cadenza almeno semestrale) sarà verificato l'ambito di trattamento consentito ai singoli incaricati o alle unità organizzative.

L'insieme delle procedure per un'idonea custodia di atti e documenti affidati agli incaricati (modalità di comportamento), nonché di atti e documenti archiviati in locali ad accesso protetto, per lo svolgimento dei relativi compiti è parte integrante della Policy in materia di trattamento dati: tali procedure riguardano l'intero trattamento dati ovvero le modalità (chi fa cosa ed in che modo) utilizzate per svolgere i propri incarichi di lavoro.
è considerato di primaria importanza l'aspetto relativo alla riconducibilità degli eventi ad un determinato soggetto. In altre parole, la vita di un documento su supporto cartaceo è costellata di eventi. Ogni evento deve poter essere, nei limiti del possibile e senza stravolgere l'operatività dell'Ente a favore di una burocrazia maniacale, essere riconducibile ad un singolo soggetto, ad un determinato momento e luogo.
Tale modalità si dimostra maggiormente utile laddove vi siano eventi pericolosi per il documento nonché per i dati in esso contenuti.

Ingresso dati nell'Ente.
Il soggetto che ritira i dati su supporto cartaceo nell'Ente deve avere cura di riporre i documenti senza aprire gli stessi, fatti salvi i casi in cui i compiti di detto soggetto non prevedano la consultazione dei documenti o attività equivalenti.
I documenti sono detenuti in mobili chiusi a chiave; la chiave deve essere in possesso unicamente del ricevente, del Responsabile d'area (vedi Policy per il trattamento con strumenti elettronici) o del Responsabile della sede.
I documenti sono trasmessi al soggetto eventualmente preposto alla loro ricezione, con modalità tali da limitare al massimo il rischio di smarrimento o trasferimento a personale non avente titolo alla ricezione di detto documento.

Archiviazione dati.
I documenti sono detenuti in mobili chiusi a chiave; la chiave deve essere in possesso unicamente del Responsabile dell'archivio, del Responsabile d'area (vedi Policy per il trattamento con strumenti elettronici) o del Responsabile della sede.

Estrazione dall'archivio per aggiornamento, consultazione, raffronto
Nel caso di grandi aziende dotate di archivi proporzionalmente dimensionati ove siano detenuti documenti riportanti dati di natura sensibile o giudiziaria, l'estrazione e la riconsegna delle pratiche è trascritta in apposito registro riportante data di ritiro della pratica, data di riconsegna della pratica, persona che ha preso in carico la responsabilità della pratica, estremi identificativi univoci della pratica.
Nel caso di aziende medio piccole e dotate di archivista, lo stesso provvede all'estrazione della pratica e monitorizza il rientro della stessa entro tempi compatibili con l'espletamento degli incarichi per i quali la pratica è stata richiesta.
Nel caso di aziende medio piccole e non dotate di archivista, l'incaricato provvede ad estrarre la pratica ed a riporre la stessa al termine dell'espletamento degli incarichi per i quali la pratica è stata ritirata.
In tutti i casi la pratica estratta dall'archivio, dovrà essere detenuta dall'incaricato al trattamento in mobili, cassetti o similari, chiusi a chiave con chiave in dotazione esclusiva all'incaricato.

Eventuale emendamento dei dati o cancellazione, distruzione degli stessi.
La distruzione dei dati nonché la cancellazione degli stessi deve seguire i dettami della normativa vigente.
Le operazioni di cancellazione, distruzione, emendamento dei dati sono poste in essere con il consenso del Responsabile al trattamento, ove eletto, o del Titolare.
I documenti, per essere considerati distrutti, dovranno subire un trattamento finalizzato a rendere impossibile l'intellegibilità dei dati in essi contenuti (a titolo esemplificativo ma non esaustivo, distruzione a mezzo distruggi documenti verticale ed obliquo).

Gli archivi cartacei contenenti dati sensibili e giudiziari sono chiusi e non accessibili al pubblico.
Nel caso in cui gli archivi cartacei fossero immagazzinati in armadi non chiudibili, gli stessi armadi dovranno essere ubicati in un'area ad accesso limitato.
Le chiavi per l'accesso a detti archivi, o relativi locali, sono in possesso di personale univocamente identificato per iscritto.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Le persone che possano accedere, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.
A tal fine verrà redatto l'insieme delle procedure che regolamenteranno l'accesso ai locali ad accesso protetto.
Quando gli archivi, o i relativi locali, non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza, le persone che vi accedono sono preventivamente autorizzate dal Responsabile dell'area, se designato, dal Responsabile del trattamento, se designato, o dal Titolare del trattamento.

Laddove possibile le modalità sopraccitate sono adottate anche per trattamenti di dati personali.

In sintesi gli incaricati al trattamento dovranno:

- informare (oralmente o per iscritto in funzione di quanto stabilito di volta in volta dal responsabile, ove designato o dal Titolare del trattamento in mancanza di quest'ultimo) circa il prelevamento di documenti dall'archivio;

- conservare, nei cassetti chiusi a chiave della propria scrivania, i documenti prelevati dall'archivio;

- non condividere e/o permettere la visione ad altri colleghi, se non per finalità strettamente correlate al trattamento stesso, dei documenti tenuti in carico;

- riporre i documenti cartacei nell'archivio non appena terminate le operazioni di trattamento o durante prolungati periodi di pausa tra una sessione di trattamento e la successiva;

- informare tempestivamente il Responsabile del trattamento, ove designato o il Titolare del trattamento in mancanza di quest'ultimo, circa eventuali anomalie riguardanti i documenti prelevati con particolare riferimento agli obblighi e doveri dettati dalla normativa e dalla policy dell'Ente in materia di trattamento dati.

Dovrà essere cura dei soggetti aventi accesso ai locali dell'archivio mantenere lo stesso ad accesso limitato curando di chiudere sempre la porta di ingresso a chiave, quando l'archivio non risulti presidiato o quando le modalità di lavoro dell'ufficio espongano a rischio le pratiche in esso contenute.

Si informa, infine, che, ai sensi dell'art.29 del Codice, il Titolare del trattamento disporrà di verifiche e controlli periodici circa la puntuale osservanza delle disposizioni di cui al presente regolamento.