Allegato al Registro dei Trattamenti del Comune di Caorle

Procedure organizzative, tecniche e fisiche adottate per la protezione dei dati personali

Il presente documento descrive le Procedure adottate dall'ente ai fini della corretta gestione dei dati personali trattati al proprio interno. Esso si pone come scopo l'adozione degli accorgimenti necessari che garantiscano la sicurezza dei dati trattati nonché la compliance alla normativa in materia. Costituisce altresì una guida per il personale interno in merito al corretto agire in situazioni che comportano il trattamento dei dati personali.

La procedure adottate sono le seguenti:

Procedura 1 – Procedure per la gestione della postazione di lavoro

Procedura 2 – Assunzione personale/Incarico di collaborazione

Procedura 3 – Formazione del personale

Procedura 4 - Regolamento sull'utilizzo degli strumenti informatici

Procedura 5 – Accesso e presa visione dei contenuti dell'account e degli strumenti informatici

Procedura 6 – Suddivisione per Unità/Aree di trattamento

Procedura 7 – Rilascio Informativa trattamento dati per ogni singolo data entry

Procedura 8 – Esercizio diritti interessati ex artt. 15 e seguenti GDPR

Procedura 9 – Sistemazione Archivi cartacei

Procedura 10 – Gestione Data Breach

Procedura 11 - Attivazione account e relativi privilegi

Procedura 12 - Indicazioni operative nella pubblicazione di atti sul sito web istituzionale

Come di seguito descritte.

Procedura 1 – Procedure per la gestione della postazione di lavoro

Nella gestione della postazione del luogo di lavoro si raccomanda di:

- Non comunicare a nessun soggetto non specificatamente autorizzato i dati personali comuni, particolari, giudiziari, sanitari e/o altri dati, elementi, informazioni di cui si viene a conoscenza nell'esercizio delle proprie funzioni e mansioni presso l'ente;
- Tenere in ordine la propria scrivania senza accatastare disordinatamente sui tavoli fascicoli, documenti e stampe. L'ordine è una misura di sicurezza preventiva contro il rischio di perdita, accesso non autorizzato di dati personali. In particolare quando si ricevono utenti o altri soggetti sincerarsi che nessun fascicolo, fotocopia o documento contenente dati personali (comuni, particolari o giudiziari), possa risaltare alla vista degli stessi; ove non fosse possibile ricevere in apposita sala riunioni, premurarsi di liberare la scrivania o capovolgere/coprire le facciate dei fascicoli e dei documenti;

- Non abbandonare presso il fotocopiatore e la stampante documenti leggibili. Maneggiare e custodire con cura le stampe di materiale riservato. Non lasciare accedere alle stampe persone non autorizzate. Se la stampante non si trova nelle vicinanze della scrivania, recarsi il più in fretta possibile a ritirare le stampe. Per stampe riservate, cercare di utilizzare una stampante non condivisa oppure la modalità di stampa ritardata impostando un tempo sufficiente a permettere il raggiungimento del dispositivo prima dell'inizio della stampa. Distruggere personalmente le stampe quando non più necessarie, oppure in caso di "brutte copie"/bozze da ristampare perché errate;
- Prestare attenzione alle fotocopie: fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Assicurarsi di non lasciare copie all'interno del dispositivo e, se necessario, per eliminare copie mal riuscite utilizzare una macchina distruggi-documenti (ove presente). Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali.
- Spegnere il computer al termine della giornata lavorativa o se ci si assenta per un periodo di tempo lungo a meno che non sia necessario lasciarlo acceso per altri motivi (aggiornamenti o accesso da remoto). Non lasciare lavori incompiuti sullo schermo. Chiudere sempre le applicazioni con cui si lavora quando si ricevono utenti o altri soggetti. Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password al momento della riattivazione. In caso ci si debba assentare dalla propria scrivania anche per pochi minuti, attivare il blocco del computer manualmente.
- Chiudere a chiave cassetti e armadi contenenti documentazione riservata. Al termine della giornata lavorativa chiudere a chiave, ove possibile, uffici o archivi se vi sono custoditi dati sanitari o giudiziari.
- Non lasciare documenti incustoditi documenti contenenti dati personali quando ci si allontana dalla postazione di lavoro;
- Non effettuare colloqui diretti con utenza o colleghi in presenza di terzi non autorizzati;
- In caso di colloqui aventi ad oggetto situazioni particolari proporre, direttamente o tramite affissione di apposito cartello informativo, all'utenza colloqui riservati in luoghi a ciò dedicati.

Procedura 2 – Assunzione personale/Incarico di collaborazione

La fase di assunzione di nuovo personale o collaboratori prevede che, all'atto di assunzione/incarico di collaborazione, vengano consegnati al nuovo dipendente/collaboratore i seguenti documenti:

a) **Contratto di assunzione/Incarico di collaborazione:** contiene gli elementi di natura contrattuale, giuslavoristica e previdenziale;
b) **Informativa sul trattamento dei dati personali ai sensi dell'art. 13 Reg. 679/16 (GDPR):** documento che specifica per quali finalità l'ente tratterà i dati personali del dipendente/collaboratore, a chi verranno comunicati gli stessi, il periodo di conservazione e le altre informazioni necessarie ai sensi dell'art. 13 GDPR. Ove previsto, viene altresì chiesto al dipendente il consenso al trattamento della propria immagine per la realizzazione di materiale audio video sul luogo di lavoro avente come finalità la promozione dell'attività svolta dall'ente, eventi realizzati o promossi, progetti, ecc. Il dipendente/collaboratore è libero di esprimere il proprio consenso.
c) **Vademecum sull'utilizzo degli strumenti informatici:** guida pratica che spiega al dipendente/collaboratore il corretto utilizzo degli strumenti informatici durante lo svolgimento dell'attività lavorativa. Per maggiori dettagli sulla misura si rinvia alla Procedura 4.
d) **Atto di nomina ad Incaricato/Addetto del trattamento dei dati personali:** ai sensi dell'art. 2 quaterdecies del D.Lgs. 196/03, ove l'attività svolta dal dipendente/collaboratore implichi il trattamento di dati personali (eventualmente anche particolari ex art. 9 e 10 GDPR), egli viene nominato incaricato del trattamento. Il presente documento serve a ricordare al

dipendente/collaboratore l'importanza dei dati personali e fornire utili istruzioni in merito al corretto agire.

Per ogni dipendente/collaboratore viene creato un apposito raccoglitore (*cartella*) informatico o cartaceo all'interno del quale vengono inserite le copie o gli estratti dei documenti suindicati.

Procedura 3 – Formazione del personale

Il personale addetto al trattamento dei dati personali, prima di iniziare la propria attività lavorativa, viene istruito in merito ai corretti comportamenti da tenere per la salvaguardia dei dati personali che egli tratterà svolgendo le proprie mansioni.

La prima modalità di formazione è la consegna/invio del Regolamento sull'utilizzo degli strumenti informatici che sarà oggetto di descrizione specifica nel prosieguo di tale documento. Il Regolamento si rivolge a tutto il personale che utilizza strumenti informatici dell'ente, senza distinzione di ruoli o incarichi. Il Regolamento è obbligatorio ed il venir meno alle disposizioni in esso contenute è punito secondo le norme in materia di diritto del lavoro.

Altra modalità di formazione è, se adottata, la nomina ad Incaricato del trattamento ai sensi dell'art. 2 quaterdecies del D.Lgs. 196/03. Come per il Regolamento sull'utilizzo degli strumenti informatici, tale documento è obbligatorio e sanzionato secondo la normativa vigente.

La formazione viene inoltre costantemente attuata attraverso specifici corsi in materia di privacy e trattamento dati personali. Tali corsi vengono effettuati da professionisti esterni qualificati che conoscono, in modo approfondito, l'ambito lavorativo dell'Ente e che sono dunque in grado di aiutare i dipendenti o collaboratori ad affrontare in modo corretto la normativa e prevenire il rischio di trattamento illecito di dati personali. Nello specifico durante la formazione si affrontano sia gli aspetti organizzativi e giuridici del GDPR, sia il corretto svolgimento delle attività pratiche effettuate dai singoli dipendenti o uffici. Tale tipologia di formazione può essere svolta anche dal Responsabile della Protezione Dati (DPO) dell'ente.

Il calendario delle attività formative svolte e di quelle successivamente programmate, è disponibile presso gli uffici amministrativi.

Procedura 4 - Vademecum sull'utilizzo degli strumenti informatici

Come anticipato sopra, a ciascun dipendente/collaboratore viene consegnato o messo a disposizione uno specifico documento contenente le regole da adottare qualora, per svolgere la propria mansione lavorativa, vengano utilizzati strumenti informatici.
Per strumenti informatici sono intesi i PC, i notebook, i cellulari/smartphone, i tablet, le stampanti, la rete internet, gli account personali, la casella di posta elettronica ed in generale qualunque mezzo elettronico o informatico fornito dall'ente per svolgere la propria mansione lavorativa. Lo scopo di tale documento è, oltre alla formazione del personale sul corretto trattamento degli strumenti e dei dati personali in essi contenuti, diminuire il rischio di intrusione nei sistemi informativi dell'Ente, di furto, distruzione o accesso non autorizzato ai dati. Nello specifico sono contenute sia disposizioni sul corretto utilizzo pratico dei dispositivi assegnati (ad es. evitare la condivisione della propria password, la corretta custodia di quest'ultima, il divieto di condivisione di documenti contenenti dati personali con persone non autorizzate, ecc), sia disposizioni di carattere generale (ad es. il divieto di navigazione su siti internet non attinenti l'attività lavorativa, il download di software senza la preventiva autorizzazione da parte dell'Amministratore di sistema, ecc).

Il Vademecum Informatico disciplina altresì la procedura di accesso da parte dell'ente, per il tramite dell'Amministratore di sistema, all'account ed agli strumenti assegnati al dipendente/collaboratore in particolari situazioni di necessità.

Procedura 5 – Accesso e presa visione dei contenuti dell'account e degli strumenti informatici

Le disposizioni adottate in merito all'accesso ed alla presa visione dei contenuti degli account e degli strumenti elettronici assegnati ai dipendenti sono state implementate alla luce dell'art. 4 della Legge 300/70 sul controllo degli strumenti di lavoro dei dipendenti, nonché in base alle linee guida del Garante Privacy per posta elettronica e internet (GU n. 58 del 10 marzo 2007) e successivi provvedimenti in materia. Tale scelta è stata effettuata in quanto al verificarsi di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale. Per tale ragione l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Preme ricordare che tutti gli strumenti informatici, gli account, la rete internet, sono stati messi a disposizione dei dipendenti e collaboratori esclusivamente per lo svolgimento delle proprie mansioni lavorative. Non sono consentite, in alcun caso, attività di natura personale.

Qualora si verifichino situazioni che incidano direttamente sulla sicurezza e la salvaguardia del sistema informatico, per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.), per tutela del patrimonio, i dipendenti e collaboratori sono informati che l'ente, tramite il proprio Amministratore di sistema, si atterrà alla procedura di seguito descritta:

i. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del Regolamento;
ii. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare l'Amministratore di Sistema ad accedere alle informazioni presenti negli account e strumenti con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP con l'identificazione del soggetto che non si attiene alle istruzioni impartite;
iii. Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti precedentemente, l'Amministratore di Sistema potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

E' altresì prevista la forma di accesso agli strumenti ed account interni per esigenze produttive e di organizzazione interna, intendendosi con ciò l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un dipendente/collaboratore. In tal caso l'ente si atterrà alla procedura di seguito descritta:

i. Redazione di un atto da parte del Responsabile Area/ufficio che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
ii. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione del dipendente/collaboratore interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;
iii. Redazione di un verbale che riassuma i passaggi precedenti.

In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

Indipendentemente dalla tipologia di accesso, qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il Regolamento sull'utilizzo degli strumenti informatici costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

Al termine del rapporto di lavoro il dipendente è consapevole che gli strumenti ed account assegnati dovranno essere riconsegnati e che ogni contenuto non lavorativo verrà eliminato. Pur ribadendo il divieto di utilizzo degli account e strumenti elettronici assegnati dall'ente per finalità non lavorative, al venir meno del rapporto di lavoro il dipendente potrà presentare specifica richiesta di estrazione e salvataggio degli eventuali contenuti personali presenti sullo strumento o account oggetto di riconsegna. La richiesta, ad insindacabile giudizio dell'ente, potrà essere o meno accettata specificando, in caso di accoglimento, le procedure e le modalità di accesso ed estrazione dei dati.

Procedura 6 – Suddivisione per Unità/Aree di trattamento

In virtù del c.d. principio di "minimizzazione dei dati" di cui all'art. 5 comma 1 lett. c del GDPR, all'interno dell'ente è stata effettuata una suddivisione in Unità o Aree di trattamento. Essa consiste una divisione del personale interno effettuate sulla base delle mansioni da ciascuno svolte. Nello specifico vengono raggruppati in Unità o Aree di trattamento i dipendenti che, per svolgere le proprie mansioni lavorative, trattano le stesse categorie di dati personali. Si potrà ad esempio ricavare l'area Direzione/Presidenza, all'interno della quale verrà inserito il personale che deve poter accedere a tutti i dati trattati dall'ente in virtù della loro posizione gerarchica. A seguire si potrà avere l'area Segreteria/Amministrazione, addetta allo svolgimento delle funzioni amministrative all'interno dell'ente, l'area Risorse Umane o Gestione del personale, ecc ecc.
Lo scopo di tale suddivisione è evitare l'accesso indiscriminato di tutto il personale interno a tutti i dati trattati dall'ente. La conseguenza è che ogni membro del personale potrà trattare solamente i dati personali indispensabili per poter svolgere le proprie mansioni lavorative. In caso di necessità ad accedere a dati ulteriori, sarà necessario rivolgere specifica richiesta al proprio Referente di area.
La suddivisione di cui sopra si traduce anche sul piano dei privilegi informatici; ogni account infatti ha, per impostazione predefinita, la possibilità di accedere solamente ai dati personali necessari della propria unità organizzativa. L'accesso a dati ulteriori e precluso dall'amministratore di sistema in fase di attivazione dell'account.
Nei casi dove sia necessario l'accesso ad aree di altri utenti, ad esempio per mansioni accavallate e/o da offrire in sostituzione, verrà fatta richiesta formale ed autorizzata dalla dirigenza competente.
Per la specifica suddivisione adottata e per l'indicazione dei Referenti di ciascuna area, si rimanda al Registro dei trattamenti (foglio 1 – Informazioni generali).

Procedura 7 – Rilascio Informativa trattamento dati per ogni singolo data entry

Come previsto dall'art. 13 GDPR, *"in caso di raccolta presso l'interessato di dati che lo riguardano",* l'ente fornisce a quest'ultimo l'informativa sulle modalità di trattamento dei dati personali.
Per adempiere ai principi dell'art. 12 GDPR secondo il quale l'informativa del trattamento dati deve essere *concisa, trasparente, intelligibile e facilmente accessibile*, l'ente ha previsto inizialmente la messa a disposizione di una prima informativa c.d. "breve". Essa, a seconda dei dati richiesti all'interessato e del servizio dall'ente reso, spiega in maniera concisa come verranno trattati i dati e per quale ragione. Vengono altresì forniti i dati di contatto del Titolare e del DPO, ove presente. Tale informativa invita l'interessato, in caso voglia avere maggiori informazioni, a prendere visione dell'informativa completa (disponibile anche sul sito web).

Il procedimento come sopra descritto viene adottato per ogni *"canale"* di entrata dei dati personali all'interno dell'ente *(data entry);* in particolare viene resa una specifica informativa sul trattamento dati in caso di:

- iscrizione a servizi ed iniziative promossi dall'ente (ad es. la newsletter effettuata tramite indirizzo e-mail o numero di telefono);
- compilazione di moduli aventi oggetto specifiche richieste effettuate dall'interessato (ad es. richiesta benefici, attestazioni, ecc);
- compilazione di form "Contattaci" o "Richiesta informazioni";
- conclusione di contratti;
- assunzione personale o procedure di selezione;
- ricezione di curricum vitae;

Tutte le informative di cui sopra sono disponibili presso gli uffici amministrativi o sul sito web nella sezione Privacy.

Procedura 8 – Esercizio diritti interessati ex artt. 15 e seguenti GDPR

In ogni momento gli interessati possono esercitare uno o più diritti previsti dal GDPR. Come specificato nelle informative sul trattamento dati, l'importante è informare l'ente di tale intenzione. Non sono previste forme rigidamente imposte per esercitare i diritti; di conseguenza sarà sufficiente anche solo mandare una mail o telefonare agli uffici amministrativi; in alternativa si può contattare il DPO. Anche il personale interno è stato adeguatamente formato per dare massima importanza e corretto riscontro all'istanza dell'interessato.

Nello specifico, qualora l'interessato scelga di esercitare i diritti di cui agli articoli 15 e seguenti del GDPR, gli verrà messo a disposizione uno specifico modulo contenente tutte le istruzioni per un'agile e corretta esecuzione della procedura di compilazione e riscontro. La compilazione del modulo si rende necessaria in quanto è essenziale essere certi sull'identità dell'interessato che esercita i diritti, per capire quale diritto stia esercitando, per dare corretto riscontro o chiedere informazioni aggiuntive ove necessario, per avere prova dell'avvenuto riscontro fornito.

Il modulo per l'esercizio dei diritti è pubblicato sul sito web dell'ente ed è liberamente scaricabile dall'interessato. Nei casi in cui quest'ultimo non abbia accesso ad internet ovvero un PC/smartphone, ci si può presentare agli uffici amministrativi e chiedere una copia gratuita.

Procedura 9 – Sistemazione Archivi cartacei

Nell'ottica di diminuzione dei rischi connessi all'accesso ed utilizzo indebito dei dati personali trattati all'interno dell'ente, qualora vi sia la necessità di conservare in forma cartacea fascicoli, contratti ed in generale ogni altro documento contenente dati personali, l'ente ha predisposto appositi armadi con funzione di conservazione cartacea.

Gli armadi non sono posizionati in zone liberamente accessibili al pubblico o ad eventuali visitatori delle strutture ma, al contrario, sono stati collocati all'interno di specifiche aree o uffici a cui abbiano accesso solamente il personale interno.

Per maggiore sicurezza, inoltre, gli armadi sono dotati di apposita serratura per evitare l'accesso e l'estrazione dei documenti da parte di soggetti non autorizzati. La custodia delle chiavi è affidata al Referente dell'area di trattamento a cui gli armadi appartengono.

Procedura 10 – Gestione Data Breach

Qualora all'interno dell'ente si verifichi una 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, si dovrà agire come di seguito indicato.

La procedura Data breach viene avviata quando si viene a conoscenza del fatto che una sospetta, presunta o effettiva violazione dei dati personali si sia verificata. Di detto evento bisogna darne immediata comunicazione al proprio Responsabile (Posizione Organizzativa o Dirigente).

Il Responsabile provvederà a dare comunicazione del sospetto, presunto o effettivo data breach a:

1. Responsabile IT (Amministratore di sistema);
2. DPO;
3. Amministratore unico e/o Referente interno;
4. Se coinvolta, la Società esterna che gestisce gli aspetti IT della risorsa violata (responsabile del trattamento ex art. 28 GDPR).

I soggetti da 1 a 3 sono definiti: "Gruppo Data Breach".

Descrizione dettagliata delle fasi:

1. Il dipendente dell'ente che si accorge di una violazione o perdita dei dati (informatici o cartacei) informa via mail il Gruppo Data Breach immediatamente relazionando quanto segue:
   a. Denominazione della/e banca/banche dati oggetto di data breach;
   b. Breve descrizione della violazione dei dati personali ivi trattati;
   c. Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati;
   d. Dove è avvenuta la violazione dei dati (ad esempio se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).
2. Il Responsabile IT e il DPO assumono eventuali ulteriori informazioni qualora ritenute necessarie.
3. Il Gruppo Data Breach procede tempestivamente alla valutazione di elementi quali:
   i. Tipo di violazione (ad es. lettura, copia, alterazione, diffusione dei dati);
   ii. Dispositivo oggetto della violazione (PC, dispositivi portativi, ecc);
   iii. Soggetti interessati dall'evento;
   iv. Gravità della violazione;
   v. Misure di sicurezza tecniche ed organizzative applicate ai dati oggetto di violazione.

Entro 12 ore dalla comunicazione (termine indicativo), effettuate le valutazioni di cui sopra, il Gruppo Data Breach dichiara motivatamente se l'evento segnalato costituisce un'effettiva violazione di dati personali come previsto dall'art. 33 e ss. GDPR. Nello specifico verrà deciso:

a) Se necessario comunicare o meno al Garante privacy l'evento di data breach;
b) Se necessario comunicare o meno agli interessati l'evento di data breach;
c) Le misure tecnologiche e organizzative assunte o da assumere per contenere la violazione dei dati e prevenire simili violazioni in futuro.

Nel caso in cui il Gruppo Data Breach **reputi necessario procedere con la comunicazione** della violazione, verrà utilizzato il modello di comunicazione predisposto dal Garante privacy disponibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9128501 . La compilazione spetterà al Titolare che, in caso di necessità, si confronterà con il DPO.
Nel caso in cui il Gruppo Data Breach **NON reputi necessario** procedere con la comunicazione della violazione, andrà compilata la "*Relazione analisi incidenti di sicurezza privacy*" (disponibile presso segreteria/uffici amministrativi) a giustificazione delle ragioni che hanno portato a non procedere con la

comunicazione dell'evento all'Autorità. Contestualmente, l'evento andrà altresì annotato all'interno del Registro delle attività di trattamento.

Procedura 11 - Attivazione account e relativi privilegi

All'interno dell'ente, per l'attivazione degli account interni e dei relativi privilegi informatici, si procede come di seguito:

1. Al momento dell'assunzione di nuovo personale viene inoltrata al Responsabile IT specifica richiesta di creazione account ed attivazione privilegi informatici da parte del Responsabile di Area/Ufficio. Tale richiesta considera la necessità, affinché il nuovo dipendente/collaboratore possa svolgere le proprie mansioni lavorative, di avere un proprio account interno.
2. Nella richiesta di cui sopra vengono indicati l'area di appartenenza del dipendente/collaboratore, i dati a cui è necessario poter accedere, i privilegi da attivare. L'amministratore di sistema procede come da richiesta.
3. Viene creato un apposito registro con l'indicazione degli account attivati e relativi privilegi. Tale registro viene periodicamente revisionato ed aggiornato.
4. Qualora venga meno il rapporto di lavoro/collaborazione, l'amministratore di sistema procede alla disattivazione dell'account ed aggiorna il relativo registro. Per la disattivazione dell'account di posta elettronica vengono seguite le disposizioni del Regolamento uso strumenti informatici in merito al periodo di "congelamento account" per esigenze organizzative interne all'ente.

Procedura 12- Indicazioni operative nella pubblicazione di atti sul sito web istituzionale

Nella pubblicazione di dati, atti e informazioni sul sito web istituzionale (albo pretorio, amministrazione trasparente ecc.) ai sensi della normativa sulla trasparenza o sulla pubblicità degli atti, gli incaricati sono informati:

- che è sempre vietata la pubblicazione di dati SANITARI O PARTICOLARI
- che la pubblicazione di dati personali identificativi è lecita solo se prevista da norma di legge o regolamento
- che se anche una norma prevede la pubblicazione di un atto, ciò non autorizza a pubblicare una copia identica all'originale detenuto dall'ufficio perché prevale il principio di minimizzazione e necessità previsto dal GDPR

Il Titolare, pertanto, fornisce agli addetti le seguenti indicazioni per la corretta pubblicazione di atti:

1) Per i provvedimenti collegiali e monocratici ed ogni altro atto oggetto di pubblicazione all'albo pretorio si raccomanda di creare una COPIA PER LA PUBBLICAZIONE, seguendo le istruzioni qui riportate:
    i. Per atti che, in riferimento a persone fisiche, NON CONTENGONO direttamente o indirettamente informazioni idonee a rivelare lo stato di salute, la vita sessuale, l'origine razziale od etnica, le condizioni religiose, filosofiche le opinioni politiche, condizioni socio economiche, stato lavorativo, la minore età, lo stato di morosità o ritardo di pagamenti, informazioni su procedimenti sanzionatori o limitativi di diritti, il fatto di non aver superato una prova selettiva o altra informazione di cui – se fossi tu al posto di quel cittadino – non saresti contento di vedere online, si consiglia di lasciare leggibili solo DATI PERSONALI IDENTIFICATIVI indispensabili (cioè nome cognome e solo eventualmente in caso di rischio omonimia la data di nascita) oscurando dati eccedenti quali Codice Fiscale, titolo di studio, impiego, indirizzo di residenza, data e luogo di nascita, dati finanziari, IBAN, punteggio analitico in caso di concorsi e altre informazioni sulla persona)

ii. Qualora invece l'atto CONTENGA le informazioni sensibili sopra descritte, è necessario TOGLIERE SEMPRE ogni riferimento identificativo delle persone fisiche, adottando tecniche di oscuramento dei dati nella copia per la pubblicazione oppure riportando i dati identificativi e ogni altra informazione identificativa in un allegato, da tenere distinto dalla determina o dall'atto (cui si potrà fare riferimento) che poi non sarà soggetto a pubblicazione

2) Per le pubblicazioni in amministrazione trasparente si invita ad effettuare le pubblicazioni limitandosi a quelle previste dal D.lgs 33/13 come esplicitate nell'allegato 1 alla delibera ANAC n. 1310/2016, attenendosi a quanto sopra descritto per le pubblicazioni all'Albo online. Si raccomanda in ogni caso di OMETTERE o OSCURARE sempre:

a) Copia di documenti di identità, immagine della grafia delle sottoscrizioni di atti, Codice Fiscale, titolo di studio, impiego, indirizzo di residenza, data e luogo di nascita, dati finanziari, IBAN, punteggio analitico in caso di concorsi e altre informazioni sulla persona fisica
b) le ditte individuali sono considerate persone fisiche ai fini privacy quindi vale quanto detto sopra per le persone fisiche, salvi gli obblighi di pubblicazione degli atti nelle procedure di gara;
c) i dati bancari non vanno mai indicati nel testo dell'atto ma vanno riportati in un allegato da tenere distinto dalla determina (cui quest'ultima potrà fare riferimento) che poi non sarà soggetto a pubblicazione.

Si consiglia di inserire nella richiesta di curriculum ovvero nelle altre dichiarazioni oggetto di pubblicazione (es. incompatibilità/inconferibilità, dichiarazione cariche incarichi ecc.) la seguente dicitura o analoga:

"Si informa che il Curriculum Vitae / dichiarazione XXX richiestoLe con la presente nota è soggetto alla pubblicazione online obbligatoria nella sezione "Amministrazione Trasparente" del sito web istituzionale, ai sensi del D.lgs 33/13. Si invita pertanto a rimuovere preventivamente ogni dato non necessario alla mera identificazione (es. numeri di telefono privati, Codice Fiscale, indirizzo di residenza ecc.) e, in caso di Curriculum, ogni altra informazione ritenuta eccedente rispetto la finalità di comprovare competenze ed esperienze relative all'incarico. Consapevole di quanto sopra, il partecipante autorizza l'ente alla pubblicazione del Curriculum inviato. Si rammenta che il Curriculum rimarrà pubblicato per i tre anni successivi alla cessazione dell'incarico e che, durante tale periodo, non è possibile richiedere l'integrazione o l'aggiornamento del Curriculum fornito."