Documento di Responsabilità

ai sensi del Regolamento UE 2016/679 in materia di protezione dei dati personali

Comune di: Loro Piceno

DOCUMENTO DI RESPONSABILITÀ (ACCOUNTIBILITY)

per le Pubbliche Amministrazioni

"Documento di responsabilizzazione e obbligo di rendicontazione" **GDPR**

General Data Protection Regulation,

RGPD Regolamento Generale della Protezione dei Dati

Il presente documento si compone di n. 28

Data di emissione: 05/06/2021

Revisione 003

Regolamento di riferimento: UE 2016/679 in materia di Protezione dei Dati personali All. 1

Legge nazionale di riferimento: Legge sulla Privacy 196/2003 Dgl. 2018/101 All. 2

Il Titolare/Delegato del Trattamento

_____ (firma leggibile)

INDICE

Premessa 3

Glossario dei termini pertinenti al DdR 4

Disposizioni PA: 10

Registro dei trattamenti –Art. 30 10

Registro della DPIA –Art. 35 12

Registro delle violazioni –Art. 33 (5) 12

Registro delle informative e consensi 13

Privacy e trasparenza on line della Pa 14

Formazione del personale 17

Regolamento per l'utilizzo della rete 18

Attività Vietate 19

Attività consentite 20

Risposta agli incidenti e Ripristino dei sistemi 21

Disposizioni di Videosorveglianza 23

Disposizioni per i siti web 24

Ciclo di vita dei dati dei Dati 26

Delibera di Consiglio comunale per l'adeguamento
al Regolamento UE 2016/679 27

PREMESSA:

Il principio di Responsabilità di cui all'articolo 5 (2) del GDPR richiede per il Titolare del trattamento, di dimostrare la conformità con i principi del GDPR. L'articolo 24 stabilisce come il Titolare del Trattamento può fare questo richiamando l'applicazione di appropriate misure tecniche e organizzative per assicurare e dimostrare che il trattamento dei dati personali sia effettuato in conformità con il GDPR.

Quindi lo scopo di questo documento è dimostrare le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati, previsti dal Regolamento UE 2016/679.

Il presente documento è stato redatto da: sindaco pro tempore/ delegato, incaricato

in qualità di delegato del Titolare del Trattamento, che provvede a firmarlo in calce e nel caso coadiuvato dal **Consulente/DPO** della protezione dei Dati: **New System Srl** via G. Brodolini 58/ b 63837 Falerone FM P.IVA 01153990443 R.E.A. 116456

Dati del Comune:

Comune di Loro Piceno, Piazza G. Matteotti, 2 -62020
Loro Piceno (MC)
P.IVA 00185360435

(da questo momento in poi chiamato PA)

Definizioni del Regolamento UE 2016/679

Ai fini del presente regolamento 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 più 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) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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;

5) «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;

6) «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;

7) «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;

8) «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;

9) «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;

10) «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;

11) «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;

12) «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;

13) «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;

14) «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;

15) «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;

16) «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;

17) «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;

18) «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;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese daquesta controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicateda 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;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensidell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

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; 23) «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;

24) «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;

25) «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);

26) «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.

Definizioni del Documento di Responsabilità

*PA: Pubblica Amministrazione

*DdR: Documento di Responsabilità

*Audit: valutazione indipendente volta a ottenere prove, relativamente a un determinato oggetto, e valutarle con obiettività, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno.

*Responsabilità (Accontibility): principio inteso a garantire che i Titolari del trattamento abbiano un controllo accurato e sono in grado di garantire e dimostrare nella pratica il rispetto dei principi di protezione dei dati. Il principio di Responsabilità (Accontibility) richiede che i Titolari del trattamento mettano in atto meccanismi e sistemi di controllo interni che garantiscano la conformità e forniscano prove - come ad esempio relazioni di *audit - per dimostrare la conformità alle parti interessate esterne, comprese le autorità di vigilanza.

*Data protection: Protezione dei dati

*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 e Particolari, 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

*Outsourcing: processo con il quale viene assegnata a un fornitore esterno la gestione di una specifica attività aziendale pertinente all'Impresa

*CLOUD: Spazio posto su dei server in rete di archiviazione dati di varie capacità e protetto da password individuale per l'accesso da qualsiasi dispositivo e da qualunque parte del mondo dove ci sia connessione internet

*Server: computer di elevate prestazioni che in una rete Internet fornisce un servizio agli altri elaboratori collegati, detti client.

*Paese terzo: paese che non è uno Stato membro dell'UE

Decisione di adeguatezza: Facoltà che ha la commissione UE di sancire che un determinato paese terzo è in grado di offrire un adeguato livello di protezione nel senso che è possibile trasferire dati a un'altra società in quel paese terzo senza che l'esportatore dei dati sia tenuto a fornire ulteriori garanzie o sia soggetto a condizioni supplementari

*rete di dispositivi: È un insieme di dispositivi hardware e software collegati l'uno con l'altro da appositi canali di comunicazione, che permette il passaggio da un utente all'altro di risorse, informazioni e dati in grado di essere pubblicati e condivisi.

*Rete Internet: rete di dispositivi a estensione mondiale, mediante la quale le informazioni contenute in ciascun dispositivo possono essere messe a disposizione di altri utenti che possono accedere alla rete stessa in qualsiasi località del mondo

*Incaricato della gestione di Sistema: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.

Incaricato della gestione delle Password: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

**Larga scala: Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; • la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento. Alcuni esempi di trattamento su larga scala sonoi seguenti:
- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast-food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

**Rif:

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE. Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO59 05/35. Sito Internet: http://ec.europa.eu/justice/data-protection/index_en.htm 16/IT WP 243 rev. 01

*DPIA: Data Protection Impact Assessment (Valutazione di impatto sulla protezione dei dati), analisi per valutare i rischi sul trattamento dei dati

*Mailing list: Elenco di indirizzi in formato elettronico per l'invio di materiale pubblicitario o informativo

*File di Log: Un log è la registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico (server, storage, client, applicazioni o qualsiasi altro dispositivo informatizzato o programma).

*Group Policy: sono un insieme di regole che controllano l'ambiente di lavoro di utenti e computer.

* cryptolocker: è virus, (una forma di ransomware) infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione.

*ransomware: è un tipo di *malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione

*Malware: indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata

Disposizioni PA

In base all'Art. 37 a) la PA deve designare un DPO:

- Designazione del responsabile della protezione dei dati (C97)

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogni qualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

- la designazione del Responsabile della protezione dei dati RPD – DPO (Data Protection Officer)

I compiti del DPO sono specificati nell'Art. 39 del Regolamento UE 2016/679:

Articolo 39

Compiti del responsabile della protezione dei dati (C97)

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il Responsabile della Protezione dei Dati (RPD-DPO) considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

- Proprietà di un Registo dei Trattamenti che soddisfi i requisiti dell'Art. 30 del Regolamento UE 2016/679 in materia di Protezione dati Personali.

Articolo 30

Registri delle attività di trattamento (C82)

All. All'interno della PA

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

(alleghiamo il "MODULO DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI" AGID: ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI).
All. 3

Precisazione:

L'art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento. Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Tali misure che non sono più minime o predeterminate comprendono:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del

trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

- **Tenere un Registro della DPIA (Art. 35). la dove è necessario**

All. 4

Le informazioni che sono in questo Registro sono di tale natura:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

-il Titolare del trattamento è comunque obbligato a tenere un registro delle violazioni dei dati personali, data breach (cd. data breach, art. 33 e 34), dove annotare anche le temporanee indisponibilità dei dati trattati

All. 5

Diagramma di flusso per la gestione della violazione dei Dati Personali

All. 6

-In caso di perdita di dati, in maniera accidentale, commessa da terzi, oppure furto (*data breach) Il Comune aderente, se ritiene che i dati archiviati possano essere divulgati e di conseguenza ledere i diritti e le libertà degli interessati, anche se non trattati su larga scala, ha l'obbligo di comunicare entro 72 ore, al Garante della Privacy, tale perdita attraverso un modulo precompilato posto on-line nel sito del Garante della Privacy,

All. 7

oppure scaricabile al Link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9128501

Esempio: I dati dei dipendenti di un'azienda tessile sono stati divulgati. I dati includevano gli indirizzi personali, la composizione della famiglia, lo stipendio mensile e le spese mediche di ciascun dipendente. In questo caso, l'azienda tessile deve informare della violazione l'autorità di vigilanza. Poiché i dati personali includono dati sensibili, come i dati relativi alla salute, l'azienda deve informare anche i dipendenti.

Esempio preso dal sito della commissione europea: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-andorganisations/obligations/what-data-breach-and-what-do-we-have-do-case-databreach_it

- Tenere i Registri che riguardano le Informative e i consensi raccolti dagli interessati

Parametri dell'informativa e consenso dell'interessato:

Definizione del Garante della Privacy sui termini informativa e consenso:

Informativa

Le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi.
L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento;
se l'interessato è obbligato o no a fornire i dati;
quali sono le conseguenze se i dati non vengono forniti;
a chi possono essere comunicati o diffusi i dati;
quali sono i diritti riconosciuti all'interessato;
chi sono il titolare e l'eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).

Consenso

Si premette che il consenso non debba essere dato se il servizio adempie ad un obbligo di legge.

(Consenso - legge - 13 gennaio 1998)

La libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare). È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad es., con la sua sottoscrizione).

- La PA, conforme con il Regolamento UE (GDPR) 2016/679 in materia di protezione dei dati, deve attraverso l'informativa e il consenso comunicare all'interessato i suoi diritti sui propri dati personali, il loro uso e le modalità di trattamento attraverso delle forme di comunicazione suddette nelle definizioni

Tali diritti sono:

1 Il diritto di essere informato su come vengono trattati i propri dati

2 Diritto di accesso ai propri dati personali

3 Diritto di rettifica dei propri dati personali

4 Il diritto alla cancellazione dei propri dati personali

5 Il diritto di limitare l'elaborazione dei propri dati personali

6 Il diritto alla portabilità dei propri dati personali

7 Il diritto di opporsi al tipo di trattamento che il Titolare sottopone per l'uso8 Diritti in relazione al processo decisionale e alla profilazione automatizzata

Requisiti per il consenso:

1. Il Titolare dei dati deve essere in grado di dimostrare chiaramente che il consenso è stato fornito dalla persona fisica interessata.
2. Il consenso non è più valido se assunto dal silenzio, inattività o caselle pre-barrate.
3. l'Interessato deve essere a conoscenza dell'identità di un Titolare dei dati, di come il Titolare possa essere facilmente contattato e anche degli scopi per i quali viene richiesto il consenso.
4. l'Interessato deve essere consapevole della reale entità, del trattamento a cui sta acconsentendo.
5. La richiesta di consenso deve essere chiaramente distinguibile da altre questioni e non sepolta all'interno di lunghe condizioni d'uso. Deve anche essere comprensibile, facilmente accessibile, chiaro e scritto in un linguaggio semplice.
6. L'Interessato può revocare il consenso in qualsiasi momento. Il consenso deve essere revocato con la stessa facilità con cui è stato dato. Questo diritto deve essere chiaramente comunicato agli interessati.
7. È necessario ottenere consensi separati per operazioni di trattamento diverse.
8. Il Titolare non è obbligato a ottenere il consenso dei dati dall'Interessato se le operazioni successive del trattamento sono "compatibili".
9. La fornitura del servizio non è subordinata al consenso del trattamento che non sia necessario per lo svolgimento del servizio fornito (Esempio: se l'Interessato si registra per ricevere un servizio di autonoleggio, il servizio non può essere rifiutato se l'Interessato ha scelto di non ricevere la newsletter dal fornitore).
10. Qualora il Titolare Raccolga il consenso da un minore (dipende gli Stati cambia da 13 a 16 anni) è tenuto a verificare che chi da il consenso al posto del minore sia veramente il genitore o chi fa le veci del minore.
11. In riferimento al consenso si fa inoltre riferimento al DECRETO LEGISLATIVO 10 agosto 2018, n. 101, Art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse p*ubblico rilevante)*

Il Comune segue le linee guida dell'Autorità di Controllo in materia di Protezione Dati Personali sulla Privacy e trasparenza on-line delle PA
"Privacy e trasparenza on line della Pa: le nuove Linee guida del Garante" scaricabile al link:
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3152130
Solo dati aggiornati e indispensabili. Vietato diffondere informazioni sulla salute. Sì agli "open data", ma senza pregiudicare i diritti delle persone. Garanzie per i più deboli

Sui siti on line della Pa solo dati esatti, aggiornati e indispensabili. Vietato diffondere informazioni sulla salute. Sì agli "open data", ma senza pregiudicare i diritti delle persone. Garanzie per i più deboli.

Allo scopo di contemperare le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali nonché la dignità delle persone, il Garante privacy ha individuato un quadro organico e unitario di cautele e misure che le PA devono adottare quando diffondono sui loro siti web dati personali dei cittadini.

Le Linee guida [doc. web n. 3134436], scaricabile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436 emanate alla luce del decreto legislativo **n.33/2013** scaricabile al link: https://www.bosettiegatti.eu/info/norme/statali/2013_0033.htm, riguardano sia la pubblicazione di dati e documenti che le Pa devono mettere on line per finalità di trasparenza, sia di quelli finalizzati a garantire altri obblighi di pubblicità degli atti amministrativi (es. pubblicazioni matrimoniali, deliberazioni sull'albo pretorio on line, avviso di deposito delle cartelle esattoriali etc.). Su tali Linee guida (in corso di pubblicazione sulla G.U.) il Garante ha sentito il Dipartimento della funzione pubblica, l'Autorità nazionale anticorruzione (Anac) e l 'Agenzia digitale.

Sintesi delle principali misure indicate per la trasparenza on line.

Principi generali

Le PA devono pubblicare solo dati esatti, aggiornati e contestualizzati.

Prima di mettere on line sui propri siti informazioni, atti e documenti amministrativi contenenti dati personali, le amministrazioni devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo.

Le PA devono pubblicare on line solo dati la cui pubblicazione risulti realmente necessaria. E' sempre vietata la pubblicazione di dati sulla salute e sulla vita sessuale. I dati sensibili (etnia, religione, appartenenze politiche etc.) possono essere diffusi solo laddove indispensabili al perseguimento delle finalità di rilevante interesse pubblico.

Occorre adottare misure per impedire la indicizzazione dei dati sensibili da parte dei motori di ricerca e il loro riutilizzo.

Qualora le PA intendano pubblicare dati personali ulteriori rispetto a quelli individuati nel decreto legislativo n.33, devono procedere prima all'anonimizzazione di questi dati, evitando soluzioni che consentano l'identificazione, anche indiretta o a posteriori, dell'interessato.

Open data e riutilizzo dei dati

I dati pubblicati on line non sono liberamente utilizzabili da chiunque per qualunque finalità.

L'obbligo previsto dalla normativa in materia di trasparenza on line della PA di pubblicare dati in "formato aperto", non comporta che tali dati siano anche "dati aperti", cioè liberamente utilizzabili da chiunque per qualunque scopo. Il riutilizzo dei dati personali non deve pregiudicare, anche sulla scorta della direttiva europea in materia, il diritto alla privacy.

Le PA dovranno quindi inserire nella sezione denominata "Amministrazione trasparente" sui propri siti web un alert con cui si informa il pubblico che i dati personali sono riutilizzabili in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto del norme sulla protezione dei dati personali.

I dati sensibili e giudiziari non possono essere riutilizzati.

Durata degli obblighi di pubblicazione

Il periodo di mantenimento on line dei dati è stato generalmente fissato in 5 anni dal decreto legislativo n.33. Sono previste però alcune deroghe, come nell'ipotesi in cui gli atti producano i loro effetti oltre questa scadenza. In ogni caso, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti hanno prodotto i loro effetti, i dati personali devono essere oscurati anche prima del termine dei 5 anni.

Motori di ricerca

L'obbligo di indicizzare i dati nei motori di ricerca generalisti (es. Google) durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza. Vanno dunque esclusi gli altri dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (es. pubblicità legale sull'albo pretorio, pubblicazioni matrimoniali etc).

Non possono essere indicizzati (e quindi reperibili attraverso i motori di ricerca) i dati sensibili e giudiziari.

Specifici obblighi di pubblicazione

Risulta proporzionato indicare il compenso complessivo percepito dai singoli dipendenti (determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione). Non è però giustificato riprodurre sul web le dichiarazioni fiscali o la versione integrale dei cedolini degli stipendi. Esistono invece norme ad hoc per gli organi di vertice politico.

A tutela di fasce deboli, persone invalide, disabili o in situazioni di disagio economico destinatarie di sovvenzioni o sussidi, sono previste limitazioni nella pubblicazione dei dati identificativi.

Vi è invece l'obbligo di pubblicare la dichiarazione dei redditi di politici e amministratori, con l 'esclusione di dati non pertinenti (stato civile, codice fiscale) o dati sensibili (spese mediche, erogazioni di denaro ad enti senza finalità di lucro etc.).

Obblighi di pubblicità degli atti per finalità diverse dalla trasparenza

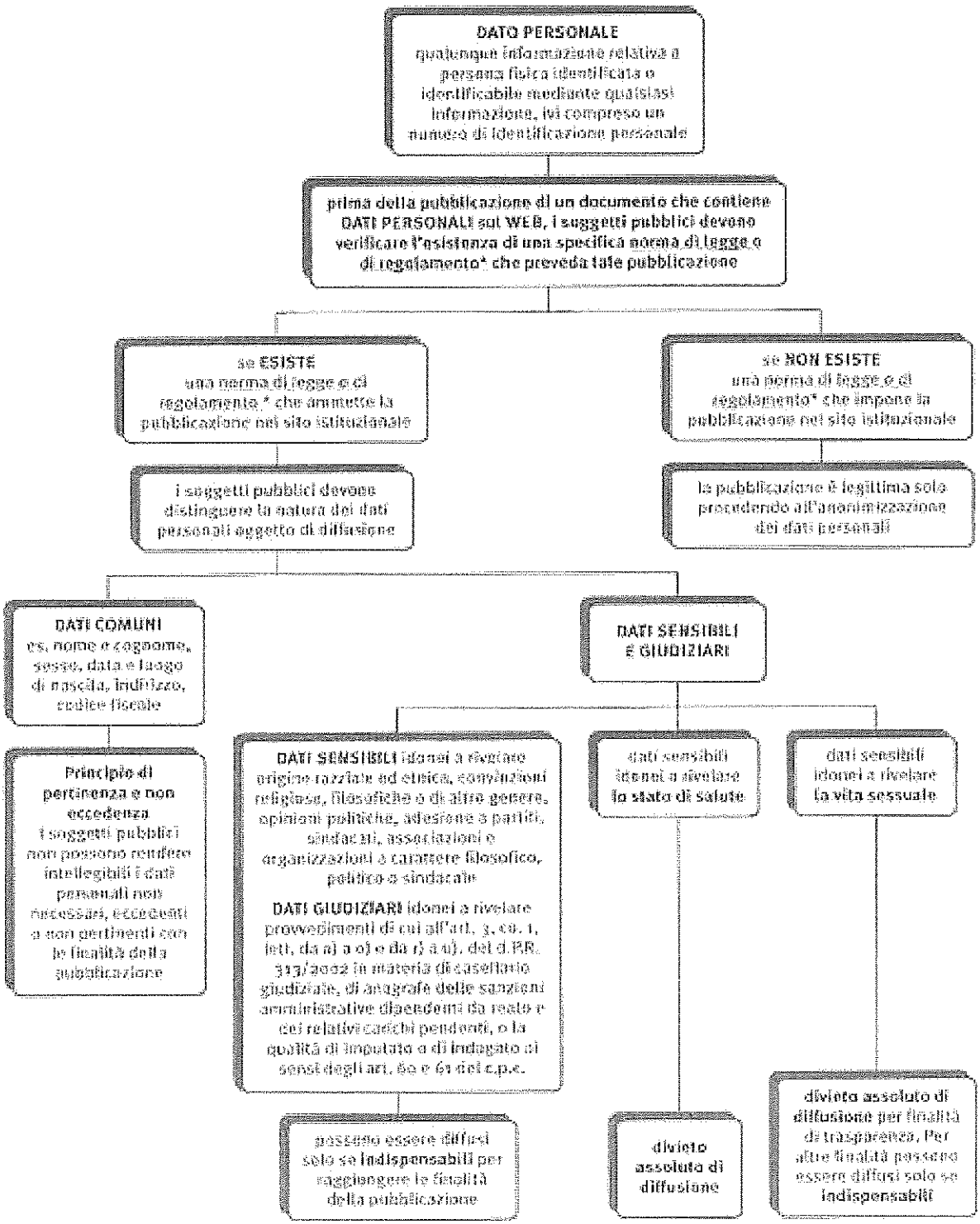
Il rispetto dei principi di esattezza, necessità, pertinenza e non eccedenza, permanenza on line limitata nel tempo dei dati personali, vale anche per la pubblicazione di atti per finalità diverse dalla trasparenza (albo pretorio on line degli enti locali, graduatorie di concorsi etc.).

Al fine di ridurre i rischi di decontestualizzazione del dato personale e la riorganizzazione delle informazioni secondo parametri non conosciuti dall'utente, è necessario prevedere l'inserimento all'interno del documento di "dati di contesto" (es. data di aggiornamento, periodo di validità, amministrazione, numero di protocollo) ed evitare l'indicizzazione tramite motori di ricerca generalisti, privilegiando funzionalità di ricerca interne ai siti web delle amministrazioni.

Deve essere evitata la duplicazione massiva dei file.

Roma, 28 maggio 2014"

Si presenta un diagramma a blocchi dell'iter per la pubblicazione dei dati personali



Formazione del personale

-Il personale deve essere formato all'ingresso del servizio, per rispettare il Regolamento UE 2016/679, e all'installazione di nuovi strumenti per il trattamento dei dati (Art. 29, Reg UE 2016/679).

-Tenere un "registro del personale" dove ci sono:

- Nome e cognome del dipendente;
- Ruolo;
- Tipo di formazione;
- Data
  - Il personale deve essere formato per rispettare il corretto uso della Posta Elettronica (e.mail)

-Tale formazione deve essere ripetuta annualmente (salvo cambiamenti strutturali e procedurali dell'Impresa)

-Il personale verrà informato e formato ogni qualvolta ci saranno aggiornamenti del GDPR -Le finalità

della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Regolamento per l'utilizzo della rete

Oggetto e ambito di applicazione

Il presente *DdR disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Principi generali – diritti e responsabilità

Il Titolare del Trattamento promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'Incaricato della gestione di sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal Titolare del

Abusi e attività vietate

Trattamento dei dati o suo delegato. Alleghiamo lo stato attuale della Rete Informatica , All.

È vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete;
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali; · rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;

· monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;

· usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;

· inserire o cambiare la password del *bios, se non dopo averla espressamente comunicata all'incaricato che amministra il sistema di rete e essere stati espressamente autorizzati dal Titolare del Trattamento;

· abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

Attività consentite

E' consentito al Titolare del Trattamento/Responsabile/ Incaricato che amministra il sistema:

· monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

· creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'Incaricato preposto darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il ***Incaricato della gestione delle password** come da procedura descritta nell'allegato (Pulsante "Proc. Password" Pg. 32) inoltre il software in dotazione da cui scaturisce il DdR gestisce con lo stesso principio suddetta procedura;

· rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

· rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Risposta agli incidenti e Ripristino dei sistemi

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il Titolare del Trattamento o con incarico assegnato il Responsabile del trattamento, l'Incaricato della sicurezza informatica, l'Incaricato della gestione di sistema nel caso in cui constatino le seguenti anomalie:

· discrepanze nell'uso degli user-id;

· modifica e sparizione di dati;

· cattive prestazioni del sistema (così come percepite dagli utenti);

· irregolarità nell'andamento del traffico;

· irregolarità nei tempi di utilizzo del sistema;

· quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente (vedi tabella A). Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'Incaricato della gestione di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il titolare del trattamento, il responsabile del trattamento e dell'Incaricato della gestione di sistema, coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response (Risposta agli incidenti e Ripristino dei sistemi), tenendo presente quanto sotto indicato:

· eseguire una copia bit to bit degli hard disk del sistema compromesso;

· se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;

· se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC **(Malicious Mobile Code)** che costituiscono la macro categoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In

tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses, il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto. **Tabella A - Procedure di spegnimento**

Sistema operativo	Azione
MS DOS	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.
UNIX/Linux	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt. 3. Se la password di root non è disponibile staccare la spina dalla presa di corrente.
Mac	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Cliccare Special. 3. Cliccare Shutdown. 4. Una finestra indicherà che è possibile spegnere il sistema. 5. Staccare la spina dalla presa di corrente.
Windows 8, Windows 10	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.

Nota: (fonte U.S. Departement of Energy)

Disposizioni di Videosorveglianza

Nell'esercitare attività di videosorveglianza, viene rispettato il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai alle 24 ore tranne particolari esigenze tecniche (fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi) o per la particolare attività rischiosa svolta mai superiore a sette giorni. La conservazione dei dati oltre il termine previsto, è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie;
- i dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.
- "Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini." Disposizione fonte
  http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3020042
- Non si può installare all'interno di un esercizio commerciale un monitor che consente la visione delle immagini a chiunque sia presente nei locali (Vedere NOTA GARANTE 17 APRILE 2014)

Disposizioni per il controllo a distanza

L'articolo 23 del Decreto Legislativo 14 settembre 2015, n. 151 ha modificato l'articolo 4 della legge n. 300/1970 (Statuto dei Lavoratori).

"Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dallar appresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, dal Ministero del lavoro e delle politiche sociali.

La disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. **Le informazioni raccolte ai sensi del primo e del secondo comma sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n.196» (Codice della privacy)". circolare INL N. 5/2018**
all. 8

Disposizioni per i siti web

- La PA deve osservare anche nei propri siti Web un atteggiamento trasparente, verso l'interessato, nel rispetto del Regolamento UE 2016/679 conforme con le disposizioni vigenti in materia di protezione dei dati personali e in linea con i parametri *dell'informativa contenuti nel Regolamento UE 2016/679 (dall'articolo 12 al 23).

- Le informazioni fornite all'interessato devono essere descritte in modo conciso, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. La lingua principale utilizzata nell'informativa deve essere quella a cui è rivolta il principale pubblico interessato (Esempio: se si vuole comunicare agli interessati di nazionalità italiana l'informativa deve essere scritta in italiano), utilizzare invece la lingua inglese se i vuole rivolgere il servizio a un mercato internazionale.

- Nei casi in cui il trattamento dei dati personali richieda il *consenso dall'interessato, il Titolare deve avere l'obbligo di dimostrare che tale consenso sia dato in maniera libera e in conformità con le prescrizioni di legge vigenti.

- L'interessato deve avere la facoltà di revocare il consenso dato, in qualsiasi momento, con la stessa facilità con cui è stato dato.

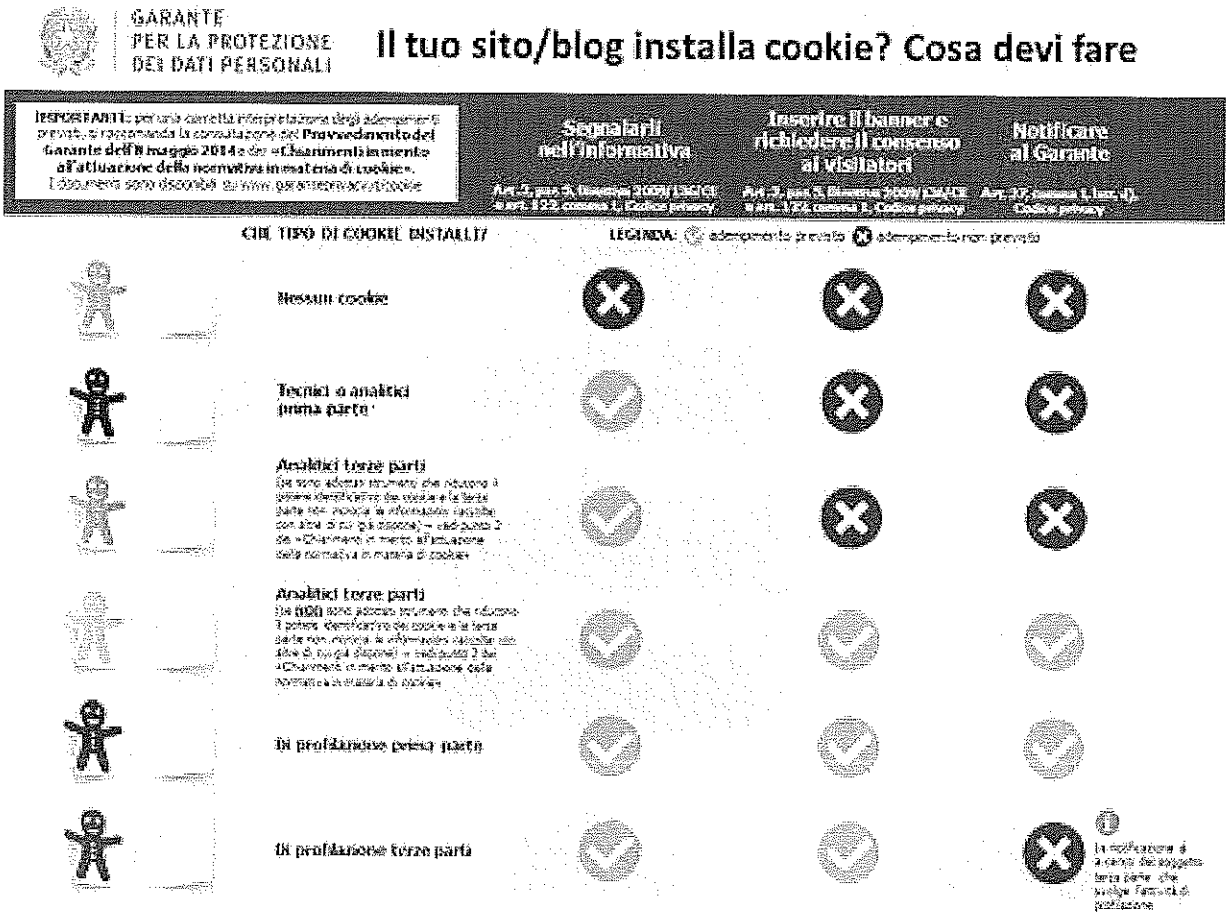
- I dati personali degli interessati rilevati dal sito seguiranno le stesse norme di sicurezza adottate da suddetto codice.

- Per una protezione adeguata dei dati dell'interessato in fase di navigazione il sito Web deve essere munito di un *protocollo di comunicazione a 128 Bit (minimo) utilizzando *certificati SSL (Secure Sockets Layer)

- Ogni sito deve avere delle informazioni, riguardanti la P.A. visibili chiare, inequivocabili, intelligibile:

- **Riferimenti DPO**
- **Albo Pretorio**
- **Policy Privacy**
- **PEC**
- **e.mail**
- **P.IVA**
- **recapiti telefonici**
- **Indirizzo**
- **nome del Comune**

Sotto riportiamo una tabella, suggerita da Garante della Privacy, con i vari tipi cookie:



Ciclo di vita dei dati dei Dati

Descriviamo di seguito con un diagramma a blocchi generico il percorso di vita dei Dati dalla Raccolta alla Cancellazione come progettazione del ciclo. Ogni Trattamento deve avere un suo ciclo come il diagramma riportato: