Comune di Porto Sant'Elpidio

Istruzioni Operative in Materia di Trattamento Dati per i soggetti autorizzati ai trattamenti dei dati personali

Allegato B

DEFINIZIONI

Ai sensi del Regolamento (UE) 2016/679, "*Regolamento generale sulla protezione dei dati*" (meglio noto come "*RGDP*" o "*GDPR*") e del D.Lgs. 196/03, recante il "*Codice in materia di protezione dei dati personali*", come modificato ed integrato dal D.Lgs. 101/18 si intende per:

a) "*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;

b) "*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;

c) "*categorie particolari di dati personali*": i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

d) "*dati giudiziari*": i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

e) "*Titolare del trattamento*": la persona fisica o giuridica (Politecnico di Torino), 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;

f) "*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;

g) "*Soggetti designati*": persone fisiche a cui il Titolare o il Responsabile del trattamento, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, possono attribuire specifici compiti e funzioni connessi al trattamento di dati personali;

h) "*persone autorizzate al trattamento*": persone fisiche autorizzate al trattamento dei dati sotto l'autorità diretta del Titolare o del Responsabile;

i) "*interessato*": la persona fisica identificata o identificabile, che può essere identificata in modo diretto o indiretto facendo riferimento, ad esempio, ad informazioni come: il nome, un numero di identificazione, dati riguardanti l'ubicazione, un identificativo on-line oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

j) "*data breach*": 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.

   Può riguardare:

   - *device* (c.d. «*IT Data Breach*»);
   - documenti cartacei *(*c.d. «*Data Breach documentale*»*)*.

INDICAZIONI GENERALI

Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti dei compiti affidati ed in conformità con le leggi ed i regolamenti in vigore.

I dati raccolti devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati; devono, inoltre, essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi stessi sono stati raccolti e successivamente trattati.

I soggetti autorizzati possono accedere unicamente ai soli archivi cartacei e/o elettronici strettamente necessari per lo svolgimento del proprio incarico e per i quali sia stato autorizzato l'accesso dal Titolare o altra figura incaricata come previsto dal Modello Organizzativo adottato dall'Ente.

Ove possibile si provvederà a ridurre al minimo l'utilizzazione e la duplicazione di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o con gestione centralizzata delle informazioni.

ISTRUZIONI INERENTI TUTTI I TRATTAMENTI

In generale, ogni persona autorizzata al trattamento dovrà:

- conformarsi a quanto stabilito dai regolamenti in materia di trattamento dei dati personali, nonché alle eventuali disposizioni in materia di sicurezza informatica;
- conformarsi alle indicazioni specifiche ricevute dal Titolare;
- raccogliere i dati presso gli interessati avvalendosi dei modelli e delle procedure predisposti dall'Amministrazione, al fine di garantire la necessaria informazione dei soggetti interessati dal trattamento dati;
- trattare i dati secondo i principi di liceità, correttezza, trasparenza, adeguatezza, pertinenza e necessità e nel rispetto delle norme di legge e dei regolamenti, per i soli fini specifici di competenza ed in maniera non eccedente rispetto agli stessi;
- controllare l'esattezza e, ove necessario, provvedere alla correzione ed all'aggiornamento dei dati trattati;
- provvedere alla cessazione del trattamento in conformità alle indicazioni ricevute dal Titolare;
- provvedere alla comunicazione ed alla diffusione dei dati personali solo nei casi previsti dalla legge e dai regolamenti;
- consentire all'interessato l'esercizio dei diritti di cui agli artt. 15 e ss. del GDPR e di quelli previsti dalla L. 241/90, in conformità con i regolamenti del Comune e dandone tempestiva comunicazione al Titolare;
- non diffondere i dati appartenenti alle categorie particolari e conservarli separatamente dagli altri dati personali;
- custodire e controllare i dati in modo da ridurre al minimo il rischio di distruzione o perdita, anche accidentale, degli stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, seguendo le indicazioni ricevute, anche in relazione alla sicurezza informatica;

  conservare sotto la propria responsabilità le credenziali di accesso attribuite, impegnandosi a non comunicarle ad altri, salvo che nei casi e con le modalità previsti dai regolamenti o indicati dal Titolare del trattamento;
- evitare qualsiasi comportamento che possa portare allo smarrimento o alla comunicazione o diffusione delle credenziali di autorizzazione;
- partecipare alle iniziative di formazione e di aggiornamento in materia di trattamento dei dati personali e di sicurezza informatica organizzati dal Titolare del trattamento;
- in caso di sospetta violazione dei dati procedere secondo quanto disciplinato dal Manuale Manuale per la gestione di una violazione di dati personali (Data Breach).

ISTRUZIONI PER I TRATTAMENTI CON STRUMENTI ELETTRONICI

Ricordando che le risorse informatiche e i servizi (quali, ad esempio, la navigazione via web e l'accesso a servizi di collaborazione in cloud) devono essere utilizzati per fini prettamente istituzionali, in relazione ai trattamenti effettuati mediante l'impiego di strumenti elettronici, ogni persona autorizzata al trattamento dovrà:

- accedere ai soli archivi (database, file, cartelle, applicativi, etc.) strettamente necessari per lo svolgimento del proprio incarico e per i quali sia stato autorizzato l'accesso dal Titolare;
- segnalare tempestivamente al proprio responsabile di struttura e agli amministratori dei sistemi/servizi IT il cambio di mansione qualora lo stesso comporti la variazione degli accessi e autorizzazioni ad archivi, applicazioni, sistemi e procedure in modo da provvedere alla disabilitazione degli accessi non più necessari;
- strutturare le password secondo le indicazioni fornite dal Titolare del trattamento dei dati e comunque non contenenti riferimenti facilmente riconducibili all'utilizzatore; provvedere a cambiare la password di accesso al proprio PC ed ai servizi informatici almeno ogni 6 mesi;
- non scrivere la propria password in luogo facilmente accessibile a terzi – ad esempio non affiggerla sul monitor del PC – né comunicarla ad altri;
- custodire tutti i supporti informatici in maniera tale da non lasciarli liberamente accessibili;
- non abbandonare la propria postazione di lavoro lasciando il terminale accessibile a terzi (es. inserire un blocca schermo o uno screensaver con password);
- mantenere aggiornato il proprio PC avendo cura che i sistemi operativi, gli antivirus e i firewall, ove previsti, siano attivi e aggiornati;
- operare affinché gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne difetti siano effettuati puntualmente;
- utilizzare l'account di posta elettronica aziendale esclusivamente per scopi professionali. Il dipendente non può condividere informazioni riservate e senza autorizzazione (ad eccezione di necessità relative alle finalità del trattamento) e non deve utilizzare la mail aziendale per scopi personali. Il Titolare ha il diritto di controllare le email dei dipendenti per verificare il regolare svolgimento delle mansioni, premesso che il controllo deve essere proporzionale e rispettare le normative sulla privacy;
- non dismettere i supporti informatici senza averli prima resi del tutto inutilizzabili chiedendo eventualmente supporto al CED;
- utilizzare per i device removibili (chiavette, hard disk esterni) e per i computer portatili e dispositivi mobili (tablet, smartphone) soluzioni, anche gratuite, di cifratura;

- segnalare tempestivamente al CED qualsiasi anomalia inerente l'accesso ai sistemi.

ISTRUZIONI PER I TRATTAMENTI CARTACEI

In relazione ai trattamenti effettuati senza l'impiego di strumenti elettronici, ogni persona autorizzata al trattamento dovrà:

- accedere ai soli archivi strettamente necessari per lo svolgimento del proprio incarico e per i quali sia stato autorizzato l'accesso dal Titolare del trattamento dati;
- controllare e custodire gli atti ed i documenti utilizzati durante le operazioni di trattamento fino alla loro restituzione, in modo che ad essi non accedano persone non legittimate;
- riporre i documenti contenenti dati personali in armadi e cassetti dotati di serrature al termine del trattamento;

  richiedere preventiva autorizzazione al Titolare ove occorra accedere ad archivi contenenti dati appartenenti alle categorie particolari o giudiziari dopo la chiusura degli archivi stessi;
- nel caso si abbia la custodia di chiavi o di altri sistemi di limitazione d'accesso agli archivi, provvedere a chiudere gli archivi alla fine della giornata lavorativa, riponendo le chiavi in maniera che non siano accessibili a terzi;
- distruggere, qualora non più necessaria, la documentazione cartacea contenente dati personali in modo tale che i contenuti non siano più consultabili ed intellegibili;
- segnalare al Responsabile Protezione Dati qualsiasi anomalia inerente l'accesso a dati personali.

ISTRUZIONI PER LO SVOLGIMENTO DELL'ATTIVITA' IN MODALITA' AGILE

In relazione ai trattamenti effettuati in modalità agile, si richiamano le precedenti istruzioni riguardanti la documentazione cartacea ed elettronica, ricordando in particolare di:

- assicurarsi che siano attivati, e vadano a buon fine, gli aggiornamenti automatici del sistema operativo del dispositivo utilizzato sia esso fornito dal Comune che personale;
- installare e tenere costantemente aggiornato un antivirus sul dispositivo;
- nel caso di apparecchiatura fornita dal Comune, garantire sempre che l'accesso alla postazione avvenga solo a seguito dell'inserimento di credenziali di accesso personali o biometriche;
- nel caso di utilizzo di un dispositivo personale, assicurarsi che i dati aziendali siano accessibili unicamente al personale, evitando la memorizzazione delle password di accesso alle risorse del Comune e adottando metodologia di cifratura dei dati salvati localmente;

- garantire che l'accesso a dispositivi ultramobili (es. smartphone, tablet) possa avvenire solo a seguito inserimento PIN, segno di riconoscimento, riconoscimento biometrico;
- non riportare le password utilizzate su *post-it* e/o su fogli lasciati in prossimità della postazione o su file non cifrati sulla postazione o su risorse di rete o servizi e sistemi cloud;
  salvare i dati preferibilmente sulle risorse di rete o in *cloud* messe a disposizione dal Comune ed evitare l'utilizzo della memoria interna dei dispositivi personali;
- limitare l'uso di chiavette USB e/o hard disk esterni per archiviare dati e documenti; in caso di necessità di utilizzo di dispositivi rimovibili, i documenti ed i dati personali devono esservi salvati in formato cifrato;
- bloccare l'accesso al dispositivo connesso a sistemi per il trattamento di dati personali in casi di assenza, seppur temporanea;
- adottare ogni cautela a protezione del dispositivo utilizzato, specialmente in caso di spostamenti;
- triturare i documenti cartacei contenenti dati personali utilizzati per l'attività lavorativa e non più necessari adottando, altresì, ogni cautela al fine di garantire la riservatezza delle informazioni trattate;
- procedere all'immediata segnalazione al CED di ogni tipo di incidente da cui potrebbe derivare una violazione di dati personali affinché si possa procedere ad adottare le misure opportune.

Procedure di backup e recupero dati

Nel presente paragrafo vengono descritte le procedure di backup che l'ente ha messo in atto per preservare i sistemi dal rischio di perdita di dati e per adempiere a quanto previsto dal GDPR Reg. UE 679/2016 in relazione alla protezione dei dati personali.

Nonostante il regolamento europeo sulla Privacy non faccia riferimento direttamente alle procedure di "Back-up" dei dati personali, esso fa parte delle misure universalmente riconosciute tra le misure di sicurezza adottate dalle aziende e dagli enti. Più specificatamente, però, le procedure di backup rientrano tra le previsioni del Capo IV Sez 2 descriventi gli Obblighi del Titolare per la Sicurezza del Trattamento, ove all'art 32 si prevede al comma 1, che il "Titolare del trattamento" e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- Infine, al comma 2, “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”.

Nel rispetto delle normative vigenti in materia di Innovazione Digitale, a seguito dell’adesione alle misure previste nel PNRR, tutti i sistemi di gestione dell’erogazione dei servizi all’utenza sono stati migrati su cloud pubblici o gestiti dai fornitori dei gestionali verticali.

E’ rimasto comunque, all’interno della sede del Municipio di Porto Sant’Elpidio, un Data Center realizzato su un’infrastruttura di virtualizzazione basata su tecnologia VmWare che ospita server virtuali per attività di storage di documenti prodotti o raccolti per fini istruttori oltre che per hosting privato di software realizzato internamente per la gestione di alcuni servizi (es.: trasporto scolastico, newsletter, emissione tagliandi invalidi, gestione fiera).

Tutti i server vengono sottoposti a procedure automatiche di salvataggio dati mentre le postazioni di lavoro dei dipendenti non sono sottoposte a procedure di backup in quanto gli stessi sono tenuti a depositare i loro dati su Server NAS (adeguatamente protetto da regole di policy e access list) o su spazio Cloud riservato ed integrato all’account di email.

L’ufficio CED si fa carico dei processi di salvataggio ed è a disposizione dell’utenza per eventuali richieste di ripristino dati.

La soluzione software utilizzata per il salvataggio dei sistemi virtuali VmWare è impostata per eseguire backup incrementali e completi ad intervalli di tempo regolari pianificati dall’amministratore di sistema.

Il Datacenter prevede che l’host dedicato a mantenere le copie di backup si trovi fisicamente su una sede diversa da quella del Municipio ed individuata alla data di produzione del presente documento presso la sala CED di Villa Murri.