APPROVATO CON DELIBERA C.C. N. 38 DEL 21/5/2018

Allegato A

PIANO OPERATIVO PRIVACY

Di seguito, sono elencate le informazioni che devono essere prese in considerazione per eseguire una corretta "mappatura" dei trattamenti posti in essere. La mappatura è consigliata per eseguire:

i. Redazione del cd. Registro del Trattamento (cfr. art. 30 GDPR - Considerando 82/89);

ii. Verifica delle misure minime di sicurezza necessarie per la tutela dei dati personali trattati (cfr. art. 32 GDPR - Considerando 29/71/83/156);

iii. Valutazione di impatto sulla protezione dei dati e consultazione preventiva con l'Autorità Garante (cd. PIA - ovvero, *Privacy Impact Assessment*) (cfr. artt. 35/36 GDPR - Considerando 84/90/91/92/93/94/95); e

iv. prevedere una specifica procedura in caso di *data breach* (cfr. artt. 33/34 GDPR - Considerando 73/86/87/88).

* * * *

Informazioni da raccogliere:

a) **identificazione delle basi giuridiche (es. contratto o obbligo di legge)** dai quali deriva un trattamento di dati personali;

b) **identificare il cd. "Interessato"** i cui dati sono o saranno oggetto di trattamento;

c) **natura/tipologia dato trattato** (cfr. art. 9 GDPR e relativi Considerando);

d) **finalità del trattamento** (cfr. artt. 9/10/11 GDPR e relativi Considerando);

e) **quali sono i dati necessari da trattare** per le finalità del trattamento. Durante il trattamento occorre sempre tenere in considerazione il principio di "minimizzazione dei dati" (cfr. art. 1c) GDPR - Considerando 39). P.S.: questa informazione è molto utile per determinare i tempi di conservazione del dato e la tutela dell'interessato e, di conseguenza, tutelare il Titolare/Responsabile del Trattamento;

f) **come vengono fornite all'interessato le informazioni relative (i) al trattamento dei suoi dati personali e (ii) all'esercizio dei propri diritti** (cfr. art. 12 GDPR e relativi Considerando). ES: modalità di consegna della "Informativa", contenuto della stessa (in particolare, molto importante è la formalizzazione dei diritti dell'Interessato) ed eventuale richiesta e ottenimento del consenso dell'Interessato;

g) **modalità e tempi di archiviazione dei dati personali**;

h) **identificare chi sono i destinatari dei dati personali** al fine di stabilire il cd. "flusso del dato" e determinare gli eventuali ruoli e responsabilità dei soggetti che prendono parte al trattamento; e

i) **verificare dove i dati personali sono conservati e se sono/possono essere trasferiti extra UE.**

* * * *

A) Prima Fase:

i. mappatura dei trattamenti e dei dati personali all'interno dei processi nei quali i dati vengono trattati. Questo è necessario per potere avere una prima bozza di registro dei trattamenti. Si tratta di un documento dove vengono mappate le informazioni principali relative ai trattamenti (tipi di dati trattati, finalità, misure di sicurezza, tempi di conservazione): il GDPR lo richiede per le aziende con più di 250 dipendenti o, ad esempio, qualora il trattamento eseguito possa presentare un rischio per i diritti e le libertà degli interessati. In ogni caso sarebbe opportuno dotarsene per avere un documento che contenga tutte le informazioni relative ai trattamenti di dati personali e che dovrà essere conservato e aggiornato in un'ottica di *accountability* (così come richiesto dal GDPR);

ii. successivamente al punto i. saranno condivise le osservazioni sulla base delle informazioni raccolte, al fine di predisporre una prima bozza di registro di trattamenti. Tale prima bozza sarà finalizzata con le ulteriori informazioni di cui si entrerà in possesso dopo aver redatto le varie procedure interne (ad esempio per l'esercizio dei diritti o per la conservazione dei dati) e stabilito la base giuridica dei vari trattamenti. Al termine di questa fase di mappatura, sarà definita anche una *gap analysis* con le azioni necessarie per l'adeguamento e che si svolgeranno durante la seconda fase;

iii. resterebbero fuori dal perimetro dell'attività legale le valutazioni sulle misure di sicurezza e le analisi dei rischi informatici connesse ai trattamenti che dovrebbero necessariamente essere svolte da tecnici.

* * * *

B) Seconda Fase:

azioni variabili da eseguirsi a valle dell'analisi eseguita durante la Prima Fase. A mero titolo esemplificativo, tali azioni potrebbero prevedere:

- redazione/revisione nomina responsabili trattamento;
- redazione/revisione nomina incaricati;
- redazione/revisione delle informative;
- revisione policy per dipendenti/professionisti per utilizzo degli strumenti elettronici;
- procedura di gestione di eventuali *data breach/data recovery*;
- verificare la nomina di Amministratore di Sistema; e
- procedura per *Data Protection Impact Assessment.*

La lista non è esaustiva e, in ogni caso, non è detto che tutte le attività elencate debbano essere eseguite: il tutto dipende dall'esito dell'analisi eseguita durante la Prima Fase.

Indirizzi e linee guida di adattamento al Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali di cui all'allegato A, parte integrante del presente provvedimento

1. TITOLARE e DESIGNATI

1. Il Comune è l'autorità pubblica titolare del trattamento dei dati ai sensi del GDPR ed esercita le proprie prerogative, poteri e doveri attraverso gli organi ed il personale dell'Ente secondo le competenze, prerogative e le responsabilità stabilite dalle disposizioni organizzative in materia ed in particolare:

- il Sindaco procede alla designazione e nomina degli organismi monocratici e collegiali previsti dalla normativa e rimessi alla determinazione del titolare con particolare riferimento al DPO-RPD, Responsabili esterni, Designati interni, gruppi di lavoro e team di progetto a supporto delle attività specifiche;
- i Dirigenti, nell'ambito delle dotazioni e risorse messe a disposizione e secondo gli indirizzi degli atti di pianificazione e programmazione comunale, adottano tutti gli atti a rilevanza esterna ivi compresi gli incarichi, affidamenti, convenzioni ed accordi per la corretta attuazione di quanto previsto dal GDPR nel rispetto della disciplina di settore con particolare riferimento alla L. 241/1990, D. Lgs 82/2005, D. Lgs 50/2016; i Dirigenti ricoprono automaticamente la funzione di organo designato dal Titolare per lo svolgimento delle relative competenze;
- il personale assegnato agli uffici e servizi svolge le funzioni di designato del titolare, senza necessità di ulteriore nomina e/o attribuzione in relazione ai trattamenti ed ai poteri/doveri

previsti dal proprio ruolo organizzativo e nel rispetto delle indicazioni formali ed informali disposte dal responsabile del servizio.

2. GRUPPO DI LAVORO GDPR

1. E' istituito un gruppo di lavoro permanente in materia di adattamento alle norme del GDPR composto da:
- segretario comunale (coordinatore e verbalizzante);
- dirigenti/Responsabili dei servizi;
- uno o più membri designati dai dirigenti in relazione alla competenza, preparazione e/o ruolo nel trattamento di dati particolari;
- almeno un referente del servizio ICT quale supporto tecnico per le problematiche di sicurezza tecnologica;
- il DPO-RPD (eventuale) invitato in occasione della trattazione di particolari tematiche.
2. Le riunioni del gruppo sono tracciate, verbalizzate e gli esiti sono resi pubblici mediante apposita sezione del sito internet comunale.
3. Il gruppo di lavoro definisce ed aggiorna in particolare:
- un programma permanente di informazione e formazione del personale;
- le priorità di intervento per l'adattamento al GDPR;
- le misure "minime" da adottare per il rispetto della normativa;
- la modulistica uniforme sia ad uso esterno che ad uso interno (informativa, consenso, comunicazioni, registri ecc...);
- la redazione e l'aggiornamento dell'elenco dei responsabili e dei designati.

3. RESPONSABILIZZAZIONE e REGISTRO DEGLI EVENTI

1. Il titolare ed i designati assicurano in ogni momento il rispetto dei principi previsti dal GDPR (art.5) dettando le opportune disposizioni organizzative e procedurali in ogni fase dell'attività.
2. Il titolare ed i designati assicurano in particolare il rispetto del principio di responsabilizzazione comprovando l'adozione di tali misure mediante la redazione ed aggiornamento di un registro degli eventi nel quale annotare tempestivamente ogni attività svolta per l'attuazione delle disposizioni del GDPR.
3. Il registro è in formato elettronico, facilmente accessibile a tutti i soggetti autorizzati alla sua redazione ed è fruibile direttamente, senza intermediazione, da parte del DPO e dell'autorità di controllo.
4: Ogni operazione, registrazione, documentazione che necessiti di essere approvata nel rispetto dei principi indicati sarà formalizzata, ove necessario, mediante protocollazione senza necessità di ulteriori formalizzazioni ove non necessarie ai sensi della vigente normativa.

4. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. Il Gruppo di lavoro cura l'aggiornamento del registro delle attività di trattamento di cui all'art.30 del GDPR, adeguando la versione iniziale di cui all'allegato B del presente atto, mediante

acquisizione dai responsabili dei servizi i dati e le informazioni sulle tipologie di trattamento secondo il modello.

2. Il registro è aggiornato tempestivamente in occasione della variazione dei trattamenti e comunque almeno una volta ogni 12 mesi.

3. Il registro è in formato elettronico, facilmente accessibile a tutti i soggetti autorizzati alla sua redazione ed è fruibile direttamente, senza intermediazione, da parte del DPO e dell'autorità di controllo.

4. Il registro, depurato di eventuali informazioni non necessarie o che possano mettere a rischio la sicurezza dell'Ente è pubblicato in rete civica nella sezione dedicata al GDPR.

6. PRINCIPIO DI COLLABORAZIONE

1. Tutto il personale coinvolto nelle procedure di trattamento dati, a qualunque livello e ruolo:

- collabora con il titolare, il DPO-RPD, l'autorità di controllo ed eventuali ulteriori soggetti addetti alla vigilanza, controllo ed attuazione delle disposizioni in materia di trattamento dei dati fornendo la massima e tempestiva collaborazione con particolare riferimento al rispetto dei principi previsti dal GDPR;
- fornisce tempestivamente informazioni su potenziali pericoli, rischi, o violazioni dei dati personali anche al fine di consentire l'esercizio dei compiti di cui all'art. 33 e 34 del GDPR (cosiddetto "data breach");
- collabora con i responsabili del trattamento, secondo le istruzioni fornite dal titolare, al fine di garantire le citate finalità e nel rispetto degli obblighi di segretezza e riservatezza.

2. Il rispetto dei principi in materia e dei compiti ed adempimenti previsti dal presente provvedimento verrà valutato in sede di raggiungimento degli obiettivi e/o negli altri casi di responsabilità del personale a vario titolo coinvolto.

Allegato B
Registro delle attività di trattamento

ALLEGATO "B"

Nominativo e contatti del Titolare del Trattamento	Nominativo e contatti dei soggetti autorizzati al Trattamento (anche definiti "Incaricati A") (cfr. art 4.10 GDPR) [da valutare]	Nominativo e contatti dei soggetti autorizzati al Trattamento (anche definiti "Incaricati B") (cfr. art 4.10 GDPR)	Nominativo e contatti delli Responsabilefi Esternofi del Trattamento
COMUNE DI PANDINO, in persona del Sindaco pro tempore, con sede in Pandino (CR), Via Castello 15	*Sig. _____ (funzionario anagrafe) (e-mail e numero di telefono dell'ufficio) [da inserire eventuali altri incaricati]*	*Sig. _____ (funzionario archivio) (e-mail e numero di telefono) [da inserire eventuali altri incaricati]*	

TRATTAMENTO	FINALITA'	CATEGORIE DI INTERESSATI	TIPOLOGIA E NATURA DEI DATI PERSONALI	CONSENSO	INFORMATIVA	TEMPI DI CONSERVAZIONE/CANCELLAZIONE DATI PERSONALI	CATEGORIE DI DESTINATARI DELLE COMUNICAZIONI DEI DATI PERSONALI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADOTTATE	NOMINATIVI DEL TITOLARE/RESPONSABILE/ INCARICATI	PAESE EXTRA UE DI TRASFERIMENTO DATI PERSONALI	GARANZIE ADEGUATE PER IL TRASFERIMENTO	DATA PROTECTION IMPACT ASSESSMENT
A) Dati personali del personale dipendente	(i) Gestione del personale dipendente nell'esercizio delle proprie mansioni lavorative e (ii) Tutela dei diritti del Comune di Pandino, ivi inclusa la relativa tutela giudiziaria, e dei cd. beni del Comune (specificare se anche di altri enti)	Personale dipendente	Dati anagrafici, dati reddituali, dati bancari, dati che rivelano l'appartenenza sindacale e lo stato di salute del personale dipendente	SI	Il modello di informativa utilizzato è qui accluso sub allegato [•] *[da verificare e completare]*	*Dieci anni dalla cessazione del rapporto di lavoro*	*Incaricati (A/B) Responsabile Esterno (es. Consulente del lavoro, Commercialista, Medico del Lavoro), [da verificare e completare]*	*[da verificare DPS + AGID]*	[•], [•], ____ [da completare] le relative nomine sono qui accluse sub allegato [•]	[da verificare]	[da verificare in base alla localizzazione dei dati]	[da verificare se eseguirla o meno, in ogni caso è consigliabile allegare la pre-verifica anche qualora l'assessment non porti alla redazione della DPIA]
B) Dati personali di consulenti terzi e fornitori	Gestione dei rapporti contrattuali intercorrenti con consulenti e fornitori e (ii) Tutela dei diritti di Comune di Pandino, ivi inclusa la relativa tutela giudiziaria, e del cd. beni del Comune (specificare se anche di altri enti)	Consulenti terzi e fornitori	Dati anagrafici, dati bancari e dati di recapito	No	Il modello di informativa utilizzato è qui accluso sub allegato [•] *[da verificare e completare]*	*[da verificare]*	*Incaricati (A/B) Responsabile Esterno (es. Consulente del lavoro, Commercialista, Medico del Lavoro), [da verificare e completare]*	*[da verificare DPS + AGID]*	[•], [•], ____ [da completare] le relative nomine sono qui accluse sub allegato [•]	[da verificare]	[da verificare in base alla localizzazione dei dati]	[da verificare se eseguirla o meno, in ogni caso è consigliabile allegare la pre-verifica anche qualora l'assessment non porti alla redazione della DPIA]
C) Dati personali specificati nei curricula inviati/consegnati ai lavoratori dipendenti del Comune di Pandino per il reclutment di aspiranti lavoratori dipendenti/collaboratori	Gestione del *recruitment* di aspiranti lavoratori dipendenti/collaboratori	Aspiranti lavoratori dipendenti/collaboratori	Dati personali non particolari	No	Il modello di informativa utilizzato è qui accluso sub allegato [•] *[da verificare e completare]*	*[da verificare]*	*Incaricati (A/B) [da verificare e completare]*	*[da verificare DPS + AGID]*	[•], [•], ____ [da completare] le relative nomine sono qui accluse sub allegato [•]	[da verificare]	[da verificare in base alla localizzazione dei dati]	[da verificare se eseguirla o meno, in ogni caso è consigliabile allegare la pre-verifica anche qualora l'assessment non porti alla redazione della DPIA]
D) Dati personali dei cittadini	Gestione dei rapporti con i cittadini per l'esercizio dei loro diritti	Cittadini	Dati anagrafici, dati relativi alla salute, dati reddituali [da verificare]	[da verificare caso per caso]	Il modello di informativa utilizzato è qui accluso sub allegato [•] *[da verificare e completare]*	*[da verificare]*	*Incaricati (A/B) Responsabile Esterno, [da verificare e completare]*	*[da verificare DPS + AGID]*	[•], [•], ____ [da completare] le relative nomine sono qui accluse sub allegato [•]	[da verificare]	[da verificare in base alla localizzazione dei dati]	[da verificare se eseguirla o meno, in ogni caso è consigliabile allegare la pre-verifica anche qualora l'assessment non porti alla redazione della DPIA]
E) Dati personali dei fornitori, delle persone fisiche che agiscono in rappresentanza dei fornitori e dei relativi dipendenti.	Svolgimento del contratto sottoscritto con fornitori	Fornitori (in caso di persone fisiche) o, qualora i fornitori siano qualificati come persone giuridiche, le persone fisiche che agiscono in rappresentanza dei fornitori e lavoratori dipendenti dei fornitori	Dati personali non particolari	[•]	[•]	*[da verificare]*	*Incaricati (A/B) Responsabile Esterno, [da verificare e completare]*	*[da verificare DPS + AGID]*	[•], [•], ____ [da completare] le relative nomine sono qui accluse sub allegato [•]	[da verificare]	[da verificare in base alla localizzazione dei dati]	[da verificare se eseguirla o meno, in ogni caso è consigliabile allegare la pre-verifica anche qualora l'assessment non porti alla redazione della DPIA]
F) Dati personali relativi a persone fisiche che non rientrano nei trattamenti da A) a E) [da verificare]	Gestione dei rapporti con terzi (persone fisiche)	Terze parti (persone fisiche)	Dati anagrafici e dati di recapito	[•]	Il modello di informativa utilizzato è qui accluso sub allegato [•] *[da verificare e completare]*	*[da verificare]*	*Incaricati (A/B) Responsabile Esterno, [da verificare e completare]*	*[da verificare DPS + AGID]*	[•], [•], ____ [da completare] le relative nomine sono qui accluse sub allegato [•]	[da verificare]	[da verificare in base alla localizzazione dei dati]	[da verificare se eseguirla o meno, in ogni caso è consigliabile allegare la pre-verifica anche qualora l'assessment non porti alla redazione della DPIA]
