COMUNE DI MARANO

CITTA' METROPOLITANA DI NAPOLI

PROGETTO DI CONFORMITA'
AL REGOLAMENTO GENERALE EUROPEO
SULLA PROTEZIONE DEI DATI PERSONALI
(679/2016)

Dott. Ing. Armando Lucci

Dicembre 2020

Codice:	679/027
Revisione:	1.00
Data di revisione:	09.12.2020
Redatto da:	Ing. Armando Lucci
Approvato da:	WebLinkComputers
Per conto:	Comune di Marano

Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica
09.12.2020	1.0	Ing. Armando Lucci	Documento base

Sommario

1. Campo d'applicazione, scopo e destinatari

Lo scopo del Piano di Progetto è definire chiaramente gli obiettivi del progetto di implementazione del Regolamento Generale Europeo sulla Protezione dei Dati (GDPR dell'UE), i documenti che devono essere scritti, le scadenze e i ruoli e le responsabilità all'interno del progetto.

Il Piano di Progetto si applica a tutte le attività svolte nel progetto di implementazione del GDPR dell'UE.

I destinatari di questo documento sono i membri dell'Ente e i membri del gruppo di progetto.

2. Documenti di riferimento

- Il GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 sulla protezione delle persone fisiche in materia di trattamento dei dati personali e sulla libera circolazione di tali dati; che abroga la direttiva 95/46 / CE
- Decreto Legislativo n. 101 del 04/08/2018
- Decreto Legislativo n. 196 del 30/06/2003

3. Progetto di Implementazione del GDPR dell'UE

3.1. Obiettivo del Progetto

Obiettivo del progetto è quello di implementare il Sistema di Gestione del GDPR del UE in conformità al Regolamento Generale sulla Protezione dei Dati (GDPR dell'UE 2016/679) del Parlamento Europeo e del Consiglio Europeo.

3.2. Risultati del Progetto

Per assicurare una pianificazione del progetto il più efficiente possibile, l'Organizzazione dovrà utilizzare il Questionario di Preparazione del GDPR per determinare quale area di conformità al GDPR necessiti di maggiore lavoro.

Durante l'implementazione del progetto del GDPR dell'UE, saranno scritti i seguenti documenti (alcuni dei quali contengono allegati che non sono espressamente riportati qui)

- **Politica sulla Protezione dei Dati Personali** – una politica intesa a stabilire i principi generali della protezione dei dati oltre a dimostrare l'impegno dell'Ente nei confronti di tali principi;
- **Politica di Protezione dei Dati dei Dipendenti –** una politica per stabilire le condizioni in cui l'Ente gestisce i dati personali dei propri dipendenti;
- **Informativa sulla Privacy** - una comunicazione per stabilire le condizioni in base alle quali l'Ente gestisce i dati personali dei propri utenti / visitatori del sito;
- **Registro delle Comunicazioni sulla Privacy -** un documento in cui è necessario elencare tutti gli avvisi pubblicati;

- **Politica di Conservazione dei Dati -** una politica per definire il periodo in cui i dati personali possono essere conservati dall'Ente;
- **Formazione del Personale –** più incontri, a scadenza pianificata, in cui si illustra il metodo e l'applicazione del GDPR;
- **Descrizione del Lavoro del Responsabile della Protezione dei Dati -** un documento che descrive le responsabilità del Responsabile della Protezione dei Dati;
- **Linee guida per l'Elenco dei Dati e la Mappatura delle Attività di Trattamento -** un documento che spiega come elencare tutte le attività relative al trattamento dei dati;
- **Elenco delle Attività di Trattamento dei Dati -** un documento destinato ad essere utilizzato dall'Ente per dimostrare la conformità ai requisiti dell'art. 30 del GDPR dell'UE;
- **Modulo di Consenso dell'Interessato** - un documento utilizzato dall'Ente per ottenere il consenso degli interessati al trattamento dei dati personali per uno scopo specifico;
- **Modulo di Recesso da parte dell'Interessato -** un documento utilizzato dagli interessati per ritirare il proprio consenso;
- **Modulo di Consenso del Titolare della Responsabilità Genitoriale-** un documento utilizzato dall'Ente per ottenere il consenso del genitore / tutore legale / rappresentante di minore per trattarne i dati personali per uno scopo specifico;
- **Modulo di Recesso del Titolare della Responsabilità Genitoriale -** un documento utilizzato dal genitore / tutore legale / rappresentante di minore per ritirare il consenso al trattamento dei dati personali per uno scopo specifico;
- **Procedura di Richiesta di Accesso ai Dati da parte dell'Interessato:** un documento per impostare il processo attraverso il quale l'Ente risponde alle richieste dei soggetti interessati;
- **Metodologia di Valutazione d'impatto sulla Protezione dei Dati -** un documento che descrive come valutare la necessità e la proporzionalità di una determinata attività di trattamento e come fornire misure per mitigare i rischi potenziali ai diritti e alle libertà degli interessati;
- **Registro della Valutazione d'impatto sulla Protezione dei Dati -** un documento utilizzato dall'Ente per documentare il processo di Valutazione d'impatto sulla Protezione dei Dati. Esso comprende il questionario di soglia e il questionario di Valutazione d'impatto sulla Protezione dei Dati;
- **Procedura di Trasferimento Transfrontaliero di Dati Peronali -** un documento per stabilire le condizioni alle quali può essere eseguito un flusso transfrontaliero di dati;
- **Clausole Contrattuali Tipo -** clausole tipo emesse dalla Commissione dell'UE per fornire adeguate garanzie in materia di tutela della vita privata e dei diritti e delle libertà fondamentali degli individui e per quanto riguarda l'esercizio dei relativi diritti.
- **Questionario di Conformità al GDPR del Processore dei dati -** un questionario inteso a valutare la conformità dei fornitori con il GDPR dell'UE;
- **Accordo con i Fornitori di Trattamento dei Dati -** un documento contrattuale inteso a stabilire i limiti e le condizioni in base al quale un fornitore (processore) può elaborare dati personali per conto della società (controllore);
- **Politica di Sicurezza IT -** descrive le regole fondamentali di sicurezza per tutti i dipendenti;
- **Politica di Controllo dell'Accesso -** definisce come la direzione approvi i diritti di accesso a particolari utenti dei sistemi informativi;
- **Procedure di sicurezza per il Dipartimento di Informatica -** descrive le regole di sicurezza che devono essere utilizzate per le infrastrutture informatiche**;**
- **Politica Bring Your Own Device (BYOD) -** descrive le regole per l'utilizzo di dispositivi mobili e di altri dispositivi**;**
- **Politica per Dispositivi Mobili e Telelavoro -** descrive le regole di sicurezza per l'utilizzo di computer portatili, telefoni cellulari e altri dispositivi al di fuori dei locali dell'Ente;

- **Politica di Clear Desk e Clear Screen -** definisce come proteggere le informazioni che si trovano sul posto di lavoro e sugli schermi del computer;
- **Politica di Classificazione delle Informazioni -** definisce come classificare i dati in base alla riservatezza e come proteggere i dati di conseguenza;
- **Politica di Anonimizzazione e Pseudonimizzazione -** definisce come utilizzare queste tecniche per proteggere l'elaborazione dei dati personali;
- **Politica sull'Uso della Cifratura -** definisce come utilizzare i controlli e le chiavi crittografiche per proteggere la riservatezza e l'integrità dei dati;
- **Piano di Disaster Recovery** - definisce come recuperare le infrastrutture e i dati dopo un incidente;
- **Procedura di Audit Interno -** definisce come verificare, stimare e valutare le garanzie organizzative e tecniche all'interno di un' Ente;
- **Allegato – Checklist per l'Audit Interno ISO 27001** fornisce una serie di domande basate sui 114 controlli elencati nell'allegato A della ISO 27001;
- **Procedura di Risposta e Comunicazione di una Violazione dei Dati -** una procedura che stabilisce gli obblighi dell'Ente in caso di violazione di dati personali;
- **Registro delle Violazioni -** Registro interno sulle violazioni dei dati;
- **Modulo di Comunicazione di una Violazione all'Autorità di Controllo -** documento da utilizzare in caso di violazione di dati
- **Modulo di Comunicazione di una Violazione agli Interessati -** documento da utilizzare in caso di violazione di dati;

3.3. Scadenze

Le scadenze per l'approvazione dei singoli documenti durante l'implementazione del GDPR dell'UE sono le seguenti:

Documento	*Scadenza per l'approvazione*
Informativa sulla Privacy	ok
Modulo di Consenso dell'Interessato	ok
Modulo di Recesso da parte dell'Interessato	ok
Descrizione del Lavoro del Responsabile della Protezione dei Dati	ok
Accordo con i Fornitori di Trattamento dei Dati	In lavorazione

La presentazione finale dei risultati del progetto è pianificata per il [data].

3.4. Organizzazione del progetto

3.4.1. Sponsor del progetto

Ogni progetto ha uno "sponsor" assegnato che non partecipa attivamente al progetto. Lo sponsor deve essere regolarmente aggiornato dal Project Manager sullo stato del progetto e intervenire nel caso in cui il progetto subisca un arresto.

Non è stato nominato Sponsor del Progetto.

3.4.2. Responsabile del Progetto

Il ruolo del Responsabile del Progetto è quello di assicurare tutte le risorse necessarie per la realizzazione del progetto, coordinare le varie fasi progettuali, informare lo Sponsor sull'avanzamento del progetto e portare avanti gli aspetti amministrativi correlati. Al Responsabile del Progetto è richiesta autorevolezza in modo da assicurare la continua implementazione del progetto nel rispetto delle scadenze previste.

Ing. Armando Lucci è stato nominato responsabile del progetto.

3.4.3. Gruppo di Progetto

Il ruolo del gruppo di progetto è seguire i vari aspetti legati alla realizzazione del progetto, al fine di rispettare le fasi specificate nello stesso e prendere tutte quelle decisioni che riguardano i vari requisiti per cui si richiede un approccio multidisciplinare. Il gruppo di progetto si incontra ogni volta prima che la versione finale di ogni documento dalla sezione 2 in poi di questo Piano di Progetto sia completato e in tutti gli altri casi in cui il responsabile del progetto lo ritenga necessario.

Tabella dei partecipanti al progetto

Nome	*Reparto Ente*	*Qualifica*	*Telefono*	*E-mail*

3.5. Principali rischi del progetto

I principali rischi nell'implementazione del progetto sono i seguenti:

1. Proroga dei termini
2. Svolgere attività che generano costi e perdite di tempo non necessari
3. Carenza o mancanza di dipendenti competenti (es. un Responsabile della Protezione dei Dati)

Le misure per ridurre i rischi sopra menzionati sono le seguenti:

- Il responsabile del progetto si assicura che tutte le attività nel progetto vengano svolte entro i termini stabiliti, e ricorre all'intervento dello sponsor di progetto in tempo utile.
- Si assume un consulente per assicurare che tempi e risorse non siano spesi in attività non importanti per il progetto, e che le attività individuali non siano condotte nella direzione errata.
- Si assume un esperto di protezione dei dati per proporre le attività più adatte.

3.6. Strumenti per l'implementazione la reportistica di progetto

Verrà creata una sezione del sito istituzionale, che contiene tutti i documenti prodotti durante il progetto. Tutti i membri del team di progetto avranno l'accesso a questi documenti. Solo il Responsabile del Progetto sarà autorizzato ad effettuare modifiche e cancellare dei file.

Il responsabile del progetto preparerà un rapporto sull'implementazione del progetto su base mensile e lo inoltrerà allo sponsor del progetto.

4. Gestione delle registrazioni sulla base di questo documento

Nome del documento	Luogo di archiviazione	Persona responsabile dell'archiviazione	Controlli per la protezione del documento	Tempo di archiviazione
Rapporto sull'implementazione del progetto (in formato elettronico)	Cartella condivisa per attività relative al progetto	Responsabile del progetto	Solo il responsabile del progetto è autorizzato a modificare i dati	Il rapporto è conservato per un periodo di 3 anni

5. Validità, durata e gestione del documento

Il presente documento ha effetto dal 09/12/2019 con una durata quinquennale. Tale durata è suscettibile a variazioni in caso di nuovi adempimenti.

Firma Responsabile Protezione Dati

_____

Firma Responsabile Trattamento Dati

_____

Titolare del Trattamento

_____