GAP ANALISYS E REMEDIATION PLANE							AGGIORNAMENTI
CTRPR001	Capo I Art. 4	Disposizioni generali	Definizioni	PARZIALMENTE ADEGUATO	In fase di audit si è riscontrata una carenza (quasi assoluta) di atti regolamentari.	**Necessario provvedere alla predisposizione dei seguenti regolamenti:** **bilanciamento Privacy e Statuto dei Lavoratori** **TIME LINE:** **31/12/2023**	Serve adozione regolamento/disiplinare sull'utilizzo degli strumenti informatici, internet e posta elettronica aggiornato al GDPR
CTRPR002	Capo II Art. 5 Comma 1-2	Principi	Principi applicabili al trattamento dei dati personali	PARZIALMENTE ADEGUATO	1.Si rileva che non è stata valutata una analisi d'impatto Privacy (DPIA). 2.**Carenza di procedura specifica su data breach** **3. Non è stata immaginata una procedura o modalità capaci di impostare sistemi di pseudonimizzazione e minimizzazione dei dati per i trattamenti ulteriori rispetto a quelli originariamente effettuati**	•Si consiglia di impostare una metodologia per la DPIA, da poter utilizzare in caso di trattamenti che prevedano il ricorso a tale istituto (Video sorveglianza con telecamere intelligenti – body scanner) •E' indispensabile predisporre procedura specifica su data breach che vada al di là di **registro dei data breach, è stato approvato anche il modello di notifica al garante ed è stata definita la procedura per informare il DPO (TIME LINE: 31/12/2022)** •Si consiglia di predisporre una procedura che contempli **pseudonimizzazione e minimizzazione dei dati per i trattamenti ulteriori rispetto a quelli originariamente effettuati** **TIME LINE:** **31/12/2023**	Con decreto in data 8.4.2021 è stato aggiornato il precedente decreto in tema di data breach, approvando la procedura di gestione degli eventi di violazione e relativi strumenti per il calcolo del livello di rischio, dando atto del nuovo modello di notifica al Garante. Su suggerimento del DPO si intende dotare l'ente di uno specifico software che agevoli la registrazione degli eventi Attività non ancora avviata.
CTRPR002	Capo II Art. 5 Comma 1-2	Principi	Principi applicabili al trattamento dei dati personali	PARZIALMENTE ADEGUATO	A seguito di intervista effettuata con il Comandante della Polizia Municipale si è evidenziata una carenza strutturale delle metodiche di trattamento in Video Sorveglianza (Video Trappole e Body scanner)	E' indispensabile predisporre uno specifico adeguamento per il trattamento in Video Sorveglianza (Video Trappole e Body scanner), che contempli: Reingegnerizzazione della centrale operativa dove allocare gli schermi di monitoraggio, con ingressi limitati ai soli autorizzati al trattamento. **TIME LINE** **31/12/2023**	Regolamento Videosorveglianza approvato con delibera CC 42/25.5.2021 esecutiva dall'1.8.2021. Predisposta e pubblicata informativa specifica. Adeguata la cartellonistica.La reingegnerizzazione della centrale operativa sarà da effettuare in occasione dello spostamento in altra sede del Comando Vigili. La reingegnerizzazione è stata immaginata in relazione allo spostamento dell'attuale sede del Comando, che attualmente è in fase di avvio.
CTRPR006	Capo II Art. 7 Comma 3	Principi	Condizioni per il consenso - Diritto di Revoca	PARZIALMENTE ADEGUATO	•non risultano in atto modalità tecnologiche e di processo strutturate che garantiscano la storicità del consenso e eventuali modifiche successive •**Non esiste un sistema automatizzato in grado di censire e gestire in maniera sincronizzata i consensi rilasciati dagli interessati**	Si suggerisce di implementare il processo di gestione delle variazioni e della revoca del consenso includendo al suo interno anche il processo di comunicazione a ciascuno dei destinatari a cui sono stati trasmessi i dati personali in merito alle rettifiche o cancellazioni o limitazioni del trattamento. **TIME LINE 31/03/2024**	Servirebbe un software per la gestione automatizzata. Da reperire sul mercato.
CTRPR007	Capo II Art. 9 Comma 1-2-3-4	Principi	Trattamento di particolari categorie di dati personali	PARZIALMENTE ADEGUATO	Si rileva l'assenza di una processo strutturato e aggiornato per la classificazione del dato privacy. Questo comporta una carenza nella misure di sicurezza adottate per le categorie particolari di dati personali.	1) Si suggerisce di effettuare un data inventory e di implementare una policy che classifichi le diverse categorie di dati privacy descrivendone le misure di sicurezza corrispondenti; 2) Si suggerisce l'implementazione di misure che garantiscano la sicurezza dei trattamenti dei dati particolari in formato cartaceo e informatico. **TIME LINE 31/12/2023**	Vedi punto **CTRPR001**
CTRPR0 20	Capo III Sezione 3 Artt. 15/22	Verifica ed implementazione	Esercizio dei diritti dell'Interessato	ADEGUATO	L'Ente ha implementato un processo per la gestione delle richieste dei diritti degli interessati.		Decreto di approvazione n. 4/2023
CTRPR022	Capo IV Sezione 1 Art. 24 Comma 1-2-3	Obblighi generali	Responsabilità del titolare del trattamento	ADEGUATO	L'Ente è in possesso di una procedura/direttiva aggiornata per la gestione della privacy che possa dimostrare l'accountability da parte del titolare rispetto alle disposizioni dettate dal Regolamento Ue 2016/679.	1) Si suggerisce l'aggiornamento e la verifica di una direttiva che documenti la metodologia per la valutazione preliminare dell'impatto dei trattamenti sulla protezione dei dati personali. In particolare, essa indirizza almeno i seguenti aspetti: - gli scenari di rischio privacy; - le metriche di valutazione del livello di rischio privacy in coerenza con quelle adottate per la valutazione di rischi ulteriori a quelli privacy (es. rischio informatico, rischio operativo, rischio di conformità, ecc.); - la soglia di rischio privacy oltre cui si rende necessario lo svolgimento di una DPIA; - il modello per lo svolgimento della DPIA; - il contenuto informativo minimo della DPIA; - le modalità di coinvolgimento del Responsabile per la protezione dei dati personali (DPO); - la soglia di rischio privacy oltre cui è necessaria una consultazione preventiva con l'Autorità di controllo; - il modello per la consultazione preventiva con l'Autorità di controllo; - i processi di aggiornamento e tenuta della DPIA; -i ruoli e le responsabilità ad alto livello per ciascuna fase dei processi di valutazione d'impatto sulla protezione dei dati e di consultazione preventiva.	Si veda regolamento privacy adottato con deliberazione di Giunta comunale dell'1 agosto 2022
CTRPR025	Capo IV Sezione 1 Art. 28 Comma 1	Obblighi generali	Responsabile del trattamento - Garanzie	ADEGUATO	All'interno dei bandi di gara per l'affidamento dei servizi che contemplano il trattamento dei dati personali di titolarità dell'Ente, vengono correttamente indicati i requisiti minimi richiesti all'aggiudicatario per la corretta tutela dei dati personali e particolari. Non sono previste, inoltre, verifiche ex post verso i responsabili esterni per testare le misure tecniche ed organizzative utilizzate per il trattamento dei dati personali (Data Processing agreement)	1) Si raccomanda di indicare già all'interno dei bandi di gara, per la selezione di fornitori di servizi che trattano o potrebbero trattare dati personali di titolarità dell'Ente, i requisiti minimi e le garanzie tecniche/organizzative per il corretto trattamento dei dati dell'Ente in modo tale da selezionare solo prestatori di servizio affidabili in tal senso. 2)Si suggerisce di implementare procedure che, previa individuazione della struttura Ente competente, garantiscano dei controlli anche ex post verso i responsabili esterni per ottenere evidenza delle garanzie da parte del fornitore esterno delle misure tecniche ed organizzative adottate per soddisfare i requisiti del Regolamento. 3)Si ritiene utile una policy su Data Processing Agreement.	Si vedano nuove procedure per nomine ex art. 28 GDPR e amministratori di sistema

CTRPR029	Capo IV Sezione 1 Art. 29	Obblighi generali	Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento - Norme per gli incaricati	ADEGUATO	L'Ente ha immaginato un percorso formativo, ma esso va erogato con livelli differenziati di approccio alla normativa italiana ed europea ed alle migliori pratiche internazionali	EROGATA FORMAZIONE VALORIALE	
CTRPR0 30	Capo IV Sezione 1 Art. 31 Comma 1	Obblighi generali	Cooperazione con l'autorità di controllo	PARZIALMENTE ADEGUATO	E' stato predisposta una procedura strutturata di cooperazione con l'autorità di controllo; i rapporti con essa vengono immaginati correttamente	1.Si raccomanda di predisporre un processo/direttiva che disciplini: - le modalità di comunicazione e reazione alle richieste effettuate dall'autorità di controllo; - le modalità di gestione delle eventuali ispezioni dell'autorità di controllo; le principali categorie di soggetti coinvolti durante le attività di cooperazione con l'autorità di controllo. **TIME LINE** **31/12/2023**	Serve procedura
CTRPR046	Capo IV Sezione 2 Art. 32	Sicurezza dei dati personali	Sicurezza del trattamento - Misure tecniche ed organizzative implementate	PARZIALMENTE ADEGUATO	**Non sono predisposte procedure e modalità tecnologiche adeguate per i trasferimenti via e-mail dei documenti contenenti dati particolari**	1) Si suggerisce di prevedere misure di sicurezza adeguate per il trattamento (trasmissione e comunicazione) dei dati relativi a condanne penali e reati sia in formato elettronico, sia cartaceo. Per il formato elettronico, si raccomanda di prevedere misure di criptazione di tali dati (statica e dinamica). 2) Si raccomanda di prevedere e far rispettare tutte le misure che assicurino la riservatezza dei documenti contenenti dati particolari/giudiziari all'interno del protocollo informatico. 3) Si raccomanda di prevedere metodi di comunicazione delle informazioni che garantiscano la sicurezza dei dati soprattutto di quelli particolari e giudiziari. In particolare, si suggerisce di utilizzare la PEC (to PEC) per l'invio di tali informazioni o di allegare alle e-mail solo file zip protetti da password (quest'ultima inviata tramite altro mezzo di comunicazione). Si raccomanda, inoltre, di redigere procedure/policy in grado di regolare, in maniera uniforme, lo scambio delle informazioni all'interno e all'esterno dell'Ente. **TIME LINE** **31/12/2023**	Vedi punto **CTRPR001**
CTRPR046	Capo IV Sezione 2 Art. 32	Sicurezza dei dati personali	Sicurezza del trattamento - Misure tecniche ed organizzative implementate	PARZIALMENTE ADEGUATO	**Non sono utilizzati strumenti di criptazione (statica/dinamica) che garantiscano la protezione di tali dati, per l'invio e la conservazione della documentazione contenente dati giudiziari**	1) Si suggerisce di prevedere misure di sicurezza adeguate per il trattamento (trasmissione e comunicazione) dei dati relativi a condanne penali e reati sia in formato elettronico, sia cartaceo. Per il formato elettronico, si raccomanda di prevedere misure di criptazione di tali dati (statica e dinamica). 2) Si raccomanda di prevedere e far rispettare tutte le misure che assicurino la riservatezza dei documenti contenenti dati particolari/giudiziari all'interno del protocollo informatico. 3) Si raccomanda di prevedere metodi di comunicazione delle informazioni che garantiscano la sicurezza dei dati soprattutto di quelli particolari e giudiziari. In particolare, si suggerisce di utilizzare la PEC (to PEC) per l'invio di tali informazioni o di allegare alle e-mail solo file zip protetti da password (quest'ultima inviata tramite altro mezzo di comunicazione). Si raccomanda, inoltre, di redigere procedure/policy in grado di regolare, in maniera uniforme, lo scambio delle informazioni all'interno e all'esterno dell'Ente. **TIME LINE** **31/12/2023**	Vedi sopra
CTRPR046	Capo IV Sezione 2 Art. 32 Comma 1-3	Sicurezza dei dati personali	Sicurezza del trattamento - Misure tecniche ed organizzative implementate	PARZIALMENTE ADEGUATO	Per l'invio e la conservazione della documentazione contenente dati giudiziari non sono utilizzati strumenti di criptazione (statica/dinamica) che garantiscano la protezione di tali dati.	1) Si suggerisce di prevedere misure di sicurezza adeguate per il trattamento (trasmissione e comunicazione) dei dati relativi a condanne penali e reati sia in formato elettronico, sia cartaceo. Per il formato elettronico, si raccomanda di prevedere misure di criptazione di tali dati (statica e dinamica). 2) Si raccomanda di prevedere e far rispettare tutte le misure che assicurino la riservatezza dei documenti contenenti dati particolari/giudiziari all'interno del protocollo informatico. 3) Si raccomanda di prevedere metodi di comunicazione delle informazioni che garantiscano la sicurezza dei dati soprattutto di quelli particolari e giudiziari. In particolare, si suggerisce di utilizzare la PEC (to PEC) per l'invio di tali informazioni o di allegare alle e-mail solo file zip protetti da password (quest'ultima inviata tramite altro mezzo di comunicazione). Si raccomanda, inoltre, di redigere procedure/policy in grado di regolare, in maniera uniforme, lo scambio delle informazioni all'interno e all'esterno dell'Ente. **TIME LINE** **31/12/2023**	Vedi sopra
CTRPR048	Capo IV Sezione 2 Art. 33 Comma 1-2-4	Sicurezza dei dati personali	Notifica di una violazione dei dati personali all'autorità di controllo - Tempistiche	ADEGUATO	Si rileva l'assenza di una procedura di gestione di eventuali violazioni dei dati personali che prevedono la notifica all'autorità di controllo e all'interessato entro i tempi richiesti dal GDPR.	Procedura Data Breach 1. Si suggerisce di implementare i processi di incident management e comunicazione degli incidenti rilevanti, integrando: - la tassonomia degli incidenti, identificando i casi in cui è riscontrata una violazione ai dati personali; - i criteri e le modalità di gestione della 'segnalazione' di una possibile violazione ai dati personali; - i criteri e le modalità di gestione della 'rilevazione e valutazione' di una possibile violazione ai dati personali; - i criteri e le modalità di gestione della 'comunicazione' di una possibile violazione ai dati personali; - le metriche per la valutazione dei rischi per gli interessati in caso di violazione ai dati personali; - le modalità operative di valutazione dei rischi per gli interessati in caso di violazione ai dati personali; - le modalità di coinvolgimento del Responsabile per la protezione dei dati personali (DPO); - i razionali che determinano la necessità di comunicare una violazione all'Autorità di controllo e ai soggetti interessati; - gli OLA (72h) per la comunicazione delle violazioni ai dati personali rilevante; - le modalità di comunicazione ed i modelli standard da utilizzare; .- i ruoli e le responsabilità ad alto livello per ciascuna fase dei processi di notifica di una violazione dei dati personali all'Autorità di controllo e di comunicazione di una violazione dei dati personali all'interessato. 2. Si suggerisce di normare nei contratti con gli outsourcer/terze parti gli obblighi, le responsabilità e gli SLA correlati alla notifica delle violazioni ai dati personali, in coerenza con i prodotti o servizi forniti e i possibili rischi afferenti al trattamento di dati personali di titolarità dell'Ente.	Con decreto in data 8.4.2021 è stato aggiornato il precedente decreto in tema di data breach, approvando la procedura di gestione degli eventi di violazione e relativi strumenti per il calcolo del livello di rischio, dando atto del nuovo modello di notifica. **E' stato previsto nel modello aggiornato e rivisto degli atti di nomina a responsabili esterni del trattamento uno specifico allegato sulla gestione dei Data Breach nel trattamento di dati di titolarità dell'Ente.**
CTRPR051	Capo IV Sezione 2 Art. 34 Comma 1-	Sicurezza dei dati personali	Comunicazione di una violazione dei dati personali all'interessato	ADEGUATO	Non risultano predisposte procedure e modalità di comunicazione delle violazione dei dati personali agli interessati senza ingiustificato ritardo	**Comunicazione agli interessati** 1. Si suggerisce di inserire all'interno della procedura inerente la gestione della violazione dei dati personali le modalità e i casi di comunicazione della violazione agli interessati come richiesto dal GDPR. La comunicazione agli interessati deve avvenire quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche e quando i dati non sono criptati. La comunicazione deve contenere: - natura della violazione; - i dati di contatto del Responsabile del trattamento; - le probabili conseguenze della violazione; le misure adottate come rimedio alla violazione.	Vedi sopra

CTRPR052	Capo IV Sezione 3 Art. 35 Comma 1-2-3-4-5-6	Valutazione d'impatto sulla protezione dei dati e consultazione preventiva	Valutazione d'impatto sulla protezione dei dati	NON ADEGUATO	Non risultano predisposte procedure e modalità per l'effettuazione delle analisi di impatto dei trattamenti svolti dal titolare	1. Si suggerisce la definizione di una procedura/direttiva che documenti la metodologia per la valutazione preliminare dell'impatto dei trattamenti sulla protezione dei dati personali. In particolare, essa indirizza almeno i seguenti aspetti: - gli scenari di rischio privacy; - le metriche di valutazione del livello di rischio privacy in coerenza con quelle adottate per la valutazione di rischi ulteriori a quelli privacy (es. rischio informatico, rischio operativo, rischio di conformità, ecc.); - la soglia di rischio privacy oltre cui si rende necessario lo svolgimento di una DPIA; - il modello per lo svolgimento della DPIA; - il contenuto informativo minimo della DPIA; - le modalità di coinvolgimento del Responsabile per la protezione dei dati personali (DPO); - la soglia di rischio privacy oltre cui è necessaria una consultazione preventiva con l'Autorità di controllo; - il modello per la consultazione preventiva con l'Autorità di controllo; - i processi di aggiornamento e tenuta della DPIA; -i ruoli e le responsabilità ad alto livello per ciascuna fase dei processi di valutazione d'impatto sulla protezione dei dati e di consultazione preventiva. **TIME LINE** **31/03/2024**	Attività da avviare.
CTRPR053	Capo IV Sezione 3 Art. 35 Comma	Valutazione d'impatto sulla protezione dei dati e consultazione preventiva	Valutazione d'impatto sulla protezione dei dati - Contenuti dell'assessment	NON ADEGUATO	Non risultano predisposte procedure e modalità per l'effettuazione delle valutazioni d'impatto dei trattamenti di dati personali	1. Si raccomanda di inserire all'interno della valutazione d'impatto DPIA le seguenti informazioni: - descrizione sistematica dei trattamenti previsti; - valutazione delle necessità/proporzionalità dei trattamenti; - valutazione dei rischi per i diritti degli interessati; - le misure previste per affrontare i rischi; **TIME LINE** **31/03/2024**	Attività da avviare.
CTRPR054	Capo IV Sezione 3 Art. 35 Comma 10	Valutazione d'impatto sulla protezione dei dati e consultazione preventiva	Valutazione d'impatto sulla protezione dei dati - Non applicabilità	NON ADEGUATO	'Non risultano predisposte procedure e modalità per l'effettuazione delle valutazioni d'impatto dei trattamenti di dati personali	Si suggerisce la definizione di una direttiva che documenti l'approccio per la valutazione preliminare dell'impatto dei trattamenti sulla protezione dei dati personali. In particolare, essa indirizza almeno i seguenti aspetti: - gli scenari di rischio privacy; - le metriche di valutazione del livello di rischio privacy in coerenza con quelle adottate per la valutazione di rischi ulteriori a quelli privacy (es. rischio informatico, rischio operativo, rischio di conformità, ecc.); - la soglia di rischio privacy oltre cui si rende necessario lo svolgimento di una DPIA; - il modello per lo svolgimento della DPIA; - il contenuto informativo minimo della DPIA; - le modalità di coinvolgimento del Responsabile per la protezione dei dati personali (DPO); - la soglia di rischio privacy oltre cui è necessaria una consultazione preventiva con l'Autorità di controllo; - il modello per la consultazione preventiva con l'Autorità di controllo; - i processi di aggiornamento e tenuta della DPIA; -i ruoli e le responsabilità ad alto livello per ciascuna fase dei processi di valutazione d'impatto sulla protezione dei dati e di consultazione preventiva. **TIME LINE** **31/03/2024**	Attività da avviare.
CTRPR055	Capo IV Sezione 3 Art. 36 Comma 1-2-3-4-5	Valutazione d'impatto sulla protezione dei dati e consultazione preventiva	Consultazione preventiva	NON ADEGUATO	Non risultano predisposte procedure e modalità per la richiesta di consultazione preventiva all'autorità di controllo all'esito di una valutazione d'impatto dei trattamenti di dati personali	1. Si suggerisce di inserire all'interno della procedura per la valutazione d'impatto DPIA la modalità per effettuare la Consultazione preventiva verso l'Autorità di controllo. In particolare la stessa deve contenere almeno: - le responsabilità dei soggetti coinvolti nel trattamento; - le finalità e i mezzi previsti - le misure per garantire i diritti degli interessati; - i dati di contatto del Titolare; - la valutazione d'impatto; **TIME LINE** **31/03/2024**	Attività da avviare.