

ALLEGATO 1

DESCRIZIONE DEL TRATTAMENTO

TITOLO SCHEDA (ED EVENTUALE NUMERO)			
1. DESCRIZIONE DEL SERVIZIO OFFERTO E DEL TRATTAMENTO CORRELATO			
Il servizio offerto dal responsabile è il seguente:			
Il trattamento di dati correlato consiste nel			
2. FINALITA' DEL TRATTAMENTO			
Il servizio ha le seguenti finalità:			
i)....			
ii).....			
3. DURATA DEL TRATTAMENTO			
La durata del trattamento è indicata nel Contratto di servizi, a cui si rimanda.			
4. TIPOLOGIA DI DATI TRATTATI			
DATI PERSONALI			
☐	Nome e cognome	☐	Luogo e data di nascita
☐	Codice fiscale	☐	Dati di contatto (indirizzo, email, telefono)
☐	Credenziali di accesso a sistemi informatici	☐	Indirizzo IP, geolocalizzazione, dati di sessione
☐	Composizione nucleo familiare	☐	ISEE
☐	Situazione patrimoniale / di reddito	☐	Situazione finanziaria
☐	Situazione economica	☐	Situazione tributaria/fiscale
☐	...	☐	
DATI PARTICOLARI E RELATIVI ALLA SALUTE			
☐	Dati inerenti origine razziale ed etnica	☐	Convinzioni religiose o filosofiche
☐	Opinioni politiche	☐	Appartenenza a sindacati
☐	Orientamento sessuale	☐	Dati biometrici
☐	Dati relativi alla salute	☐	Dati relativi a condanne penali
☐	...	☐	...
In alternativa alla descrizione tabellare precedente, si possono descrivere i dati in forma discorsiva nel presente documento.			
5. CATEGORIE DI INTERESSATI			
☐	Cittadini	☐	Contribuenti e loro familiari
☐	Amministratori e loro familiari	☐	Partecipanti a bandi di concorso
☐	Personale che opera a vario titolo presso l'ente e loro familiari		
☐	Soggetti che fruiscono del servizio erogato dal Titolare		
☐	Soggetti i cui dati sono trattati per obbligo di legge correlato al procedimento		
In alternativa alla descrizione tabellare precedente, si possono descrivere i dati in forma discorsiva nel presente documento.			
6. ELENCO DEI SUB-RESPONSABILI AUTORIZZATI			
DENOMINAZIONE		FUNZIONE SVOLTA	
....			
....			
7. ELENCO DEGLI AMMINISTRATORI DI SISTEMA [FACOLTATIVO]			

NOME E COGNOME	FUNZIONE SVOLTA
....	
....	
8. INFRASTRUTTURE E DATI TRATTATI DAL RESPONSABILE [FACOLTATIVO]	
SPECIFICARE QUALI INFRASTRUTTURE SONO MESSE A DISPOSIZIONE DAL RESPONSABILE (ES PIATTAFORMA SOFTWARE, SERVIZIO IN CLOUD, ECC) E QUALI INFORMAZIONI VENGONO TRATTATE (ES DATI DEI TRIBUTI, DATI RACCOLTI DALLA PIATTAFORMA FORNITA, ECC)	
9. ARCHIVI DEL TITOLARE A CUI ACCEDE IL RESPONSABILE[FACOLTATIVO]	
SPECIFICARE SE IL FORNITORE ACCEDE AD ARCHIVI MESSI A DISPOSIZIONE DEL TITOLARE PER LO SVOLGIMENTO DEL SERVIZIO, (ES. LA BANCA DATI ANAGRAFICA, I DATI DEL CATASTO, DOCUMENTAZIONE CARTACEA, ECC)	
10.RILASCIO DELL'INFORMATIVA (FACOLTATIVO)	
Il responsabile è tenuto al rilascio dell'informativa agli interessati nei contenuti, forme e modalità concordati con il titolare.	
11.RIFERIMENTI E DATI DI CONTATTO	
SOGGETTO	RIFERIMENTI
REFERENTE DEL TITOLARE	
RESPONSABILE PROTEZIONE DATI PERSONALI DEL TITOLARE	Email:
REFERENTE DEL RESPONSABILE	
RESPONSABILE PROTEZIONE DATI PERSONALI DEL RESPONSABILE	Email:

ALLEGATO 2

ISTRUZIONI E MISURE DI SICUREZZA DA ADOTTARE

Le prescrizioni riportate nella seguente tabella costituiscono specifiche istruzioni sul trattamento dei dati effettuato per conto del titolare del trattamento. Le disposizioni sono tassative e la loro mancata osservazione comporta una violazione delle disposizioni normative e contrattuali relative al contratto di servizio in essere tra il titolare e il responsabile.

1. MISURE ORGANIZZATIVE
a. Tenuta di un registro delle attività del trattamento come previsto dall'art. 30 RGPD, in cui siano riportati i trattamenti effettuati per conto del titolare
b. Presenza di una procedura di gestione degli incidenti che preveda, nei casi si renda necessario, la sollecita segnalazione al titolare secondo le disposizioni definite nell'accordo fra le parti
c. Nomina di un Data Protection Officer
d. Conferimento di istruzioni scritte ai soggetti autorizzati dal responsabile in tema di protezione e sicurezza dei dati personali
e. Formazione dipendenti in tema di protezione e messa in sicurezza dei dati trattati nello svolgimento di attività correlate al servizio svolto per conto del titolare
f. Formalizzazione per tutti i dipendenti e collaboratori del responsabile di un impegno alla riservatezza sui dati trattati nello svolgimento di attività correlate al servizio svolto per conto del titolare
g. Ricorso a sub-responsabili solo a seguito di preventiva comunicazione al titolare e a sua mancata opposizione entro 30 giorni dalla sua comunicazione
h. Limitazione ai sub-responsabili di accesso ai dati del titolare espressamente per l'espletamento dei servizi oggetto dell'accordo tra titolare e responsabile
i. Verifiche periodiche sui fornitori (ad es. tramite verifica documentale, verifica presenza e/o sussistenza certificazioni del fornitore o audit presso il fornitore)
j. Espresso divieto di trasferimento dati verso un paese terzo o un'organizzazione internazionale che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.)
k. Trasferimento o effettuazione di trattamento dei dati personali del titolare verso un paese terzo e/o al di fuori dell'Unione Europea esclusivamente a seguito di autorizzazione scritta del Titolare
2. MISURE FISICHE
a. Presenza di sistemi di protezione degli ambienti in cui viene effettuato il trattamento dei dati per conto del titolare (es. allarmi perimetrali o volumetrici, presenza di inferriate o blindatura alle finestre e porte antisfondamento, sistemi antincendio)
b. Presenza di sistemi di limitazione degli accessi ai soli soggetti autorizzati agli ambienti in cui viene effettuato il trattamento dei dati per conto del titolare (es. tramite accessi con chiavi/badge, monitoraggio/tracciamento degli accessi, guardiania, ecc)
c. Adozione di policy e procedure per la gestione degli accessi fisici ai locali in cui viene effettuato il trattamento dei dati per conto del titolare
d. Protezione fisica e conservazione in sicurezza dei supporti portatili di archiviazione in uso presso l'organizzazione
3. MISURE SUGLI ARCHIVI CARTACEI
a. Messa in sicurezza degli archivi cartacei attraverso i quali viene effettuato il trattamento dei dati per conto del titolare
b. Limitazione degli accessi agli archivi cartacei (es. mediante chiusura a chiave degli armadi e/o degli uffici in assenza del personale, etc...)

c. Condivisione e della comunicazione cartacea esclusivamente con soggetti autorizzati
d. Comunicazione a terzi di documentazione cartacea solamente quando previsto all'interno delle attività di trattamento di dati effettuato per conto del titolare
e. Conferimento dell'informativa agli interessati se previsto tra le condizioni di fornitura del servizio
4. MISURE SULLE RISORSE ICT
a. Adozione di procedure e sistemi di gestione degli accessi logici (sistemi e processi di autorizzazione, profilazione degli accessi, gestione delle utenze, verifica periodica di sussistenza dei diritti di accesso dei soggetti autorizzati con disabilitazione delle utenze non più operanti)
b. Implementazione di sistemi e processi di salvataggio (backup) e ripristino dei dati trattati per conto del titolare (schedulazione periodica dei backup in ambiente separato dalla rete di produzione, test di ripristino, custodia dei supporti e dispositivi di backup in luoghi sicuri)
c. Limitazione di utilizzo esclusivo di software autorizzati dall'organizzazione per il trattamento di dati personali, con divieto di utilizzo di risorse non autorizzate
d. Adozione di procedure di dismissione e/o eliminazione di dispositivi e supporti hardware contenenti dati del titolare
e. Ove necessario, adozione di tecniche di cifratura e/o pseudonimizzazione degli archivi informatici
f. Adozione di sistemi antimalware per postazioni di lavoro, server e altri dispositivi elettronici di trattamento dati
g. Implementazione di processi e sistemi di verifica di vulnerabilità sui sistemi e di distribuzione delle patch di sicurezza rilevanti sui dispositivi in uso presso l'organizzazione
h. Aggiornamento continuo dei livelli di sicurezza dei sistemi informatici in uso presso l'organizzazione con cui si trattano dati per conto del titolare
i. Impiego di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise)
j. Effettuazione di audit periodici tramite organizzazioni esterne specializzate sui propri sistemi di sicurezza (es. vulnerability assessment, penetration test, security assessment, ecc.)
k. Attivazione di sistemi di cifratura sui canali di connessione esterna autorizzata alla rete dell'organizzazione (es. Virtual Private Network o strumenti equivalenti)
l. Implementazione di sistemi di protezione, autorizzazione, autenticazione e crittografia sulle reti wireless utilizzate presso l'organizzazione
m. Attivazione di sistemi di cifratura sui dispositivi portatili che trattano dati personali
n. Adozione ed osservanza delle Misure Minime di Sicurezza ICT per le PA, almeno per il livello M ("Minimo"), sui sistemi informativi attraverso cui sono trattati i dati per conto del titolare del trattamento
o. Distruzione e smaltimento dei supporti informatici di memorizzazione logica o cancellazione dei dati (o attuazione di misure atte a garantire la loro non intelligibilità) presenti sui supporti per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici
5. MISURE SULLE CREDENZIALI DI ACCESSO
a. Definizione di politica di gestione delle password (password complesse con caratteri alfanumerici, lunghezza di almeno 12 caratteri, scadenza con obbligo di modifica della password ogni 3 mesi, reimpostazione password obbligatoria al momento della comunicazione)
b. Comunicazione agli utenti di userid e password utilizzando differenti canali di comunicazione
c. Assegnazione di credenziali personali ad ogni utente
d. Divieto di condivisione di credenziali fra gli utenti autorizzati e di comunicazione ad altri

soggetti delle credenziali personali
e. Conservazione in sicurezza delle credenziali assegnate
f. Istruzione agli autorizzati circa la messa in sicurezza delle proprie credenziali
g. Blocco delle utenze in caso di tentativi ripetuti di inserimento di credenziali scorrette
6. MISURE SUGLI AMMINISTRATORI DI SISTEMA
a. Individuazione e designazione individuale degli amministratori di sistema dei soggetti che svolgono le attività di gestione e manutenzione dei sistemi informatici, definite dal provvedimento del Garante Privacy del 2008 in tema di amministratori di sistema
b. Individuazione degli specifici ambiti di operatività degli amministratori di sistema autorizzati in base al profilo di operatività assegnato
c. Attribuzione di credenziali specifiche, con obbligo di utilizzo di password con lunghezza di almeno 14 caratteri per tutti i profili di amministrazione dei sistemi informatici attraverso i quali vengono trattati i dati del titolare del trattamento
d. Aggiornamento continuo dell'elenco degli amministratori di sistema che operano sulle risorse attraverso cui sono trattati i dati del titolare del trattamento
e. Tracciamento e registrazione diretta o indiretta degli accessi degli amministratori di sistema sui sistemi gestiti dal responsabile, con mantenimento per almeno 6 mesi dei log di accesso ai sistemi
f. Adozione ed osservanza delle Misure Minime di Sicurezza ICT per le PA, almeno per il livello M ("Minimo"), per gli ambiti di propria competenza in materia di amministratori di sistema
7. MISURE DI SICUREZZA SUI CENTRI ELABORAZIONE DATI
a. Limitazione, monitoraggio e tracciamento degli ingressi/uscite tramite controllo degli accessi fisici ai locali da parte dei soggetti autorizzati (attraverso l'utilizzo di credenziali, dispositivi di autenticazione o identificazione personale)
b. Presenza di adeguati sistemi di protezione fisica dei locali (es. porte antisfondamento, finestre blindate o protette da inferriate)
c. Installazione di sistemi di controllo antintrusione (telecamere interne o sistemi volumetrici)
d. Presenza di adeguati sistemi di protezione ambientale dei locali (sistema di rilevamento fumi e/o sistema antincendio allarmato, sistema di rilevamento allagamento allarmato, sistema di rilevamento temperatura allarmato, sistema di condizionamento)
e. Presenza di sistemi di continuità elettrica costituiti da UPS di zona e, in caso di necessità, gruppi elettrogeni
f. Adozione di sistemi di ridondanza delle risorse ICT (elaboratori di dati, sistemi di comunicazione e trasmissione, dispositivi di archiviazione)
g. Adozione di procedure e sistemi di disaster recovery e business continuity
8. MISURE DI SICUREZZA SUL SOFTWARE
a. Progettazione e sviluppo del software con tecniche di <i>security by design</i> e <i>security by default</i>
b. Implementazione di specifiche di sicurezza nel codice, nella struttura della base dati e nei sistemi di autenticazione degli utenti
c. Adozione di tecniche di cifratura e/o pseudonimizzazione sulle basi di dati in caso di trattamento di categorie particolari di dati o dati personali relativi a condanne penali e reati
d. Effettuazione di test periodici di sicurezza sul software sviluppato (es. penetration test, security assessment, ecc.)
e. Valutazione e correzione continua delle vulnerabilità sul software fornito