ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI
Art. 28 Regolamento Europeo 2016/679
tra

Il Comune di Baiso, con sede legale a *Baiso (RE) Piazza della Repubblica n. 1*, C.F. 80019170358 e P.IVA 00237240353 (di seguito anche **"Titolare del trattamento"** o **"Titolare" o "Ente"**), rappresentato ai fini del presente accordo *[indicare nome e cognome di chi sottoscrive l'accordo]* in qualità di Responsabile del Servizio *[indicare il Settore]*,

e

*[indicare denominazione/ragione sociale del soggetto terzo che sottoscrive l'accordo]***,** con sede legale *[indicare indirizzo sede legale del soggetto terzo, Comune e Provincia]*, C.F. e P.IVA *[indicare C.F. e P. IVA del soggetto terzo]* (di seguito anche **"Responsabile del trattamento" o "Responsabile"**), rappresentata ai fini del presente accordo da *[indicare nome e cognome del rappresentante del soggetto terzo che sottoscrive l'accordo]*, in qualità di *[indicare, ad esempio, se rappresentante legale, Dirigente, ecc ecc…]*,

Premesso che

a) *[inserire, anche scomponendo in più punti, i riferimenti da cui trae origine il rapporto contrattuale/convenzionale/accordo in virtù dei quali il soggetto terzo deve trattare dati personali per conto dell'Ente, come ad esempio la determina di aggiudicazione, il relativo contratto, l'accordo, la convenzione];*
b) Il Regolamento UE 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati) **[di seguito anche "Regolamento"]**, consentono a qualsiasi Titolare del trattamento dei Dati Personali di ricorrere ad uno o più Responsabili che trattano dati per conto del Titolare stesso, a condizione che tali soggetti presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato;

si conviene e si stipula quanto di seguito riportato.

1. Valore delle premesse e invariabilità dell'Accordo

Le premesse formano parte integrante e sostanziale del presente Accordo e ad esse le Parti intendono attribuire valore negoziale.
Le parti si impegnano a non modificare l'Accordo se non per aggiungere o aggiornare informazioni negli allegati.
Ciò non impedisce alle parti di includere quanto indicato nel presente Accordo in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, il presente Accordo o ledano i diritti o le libertà fondamentali degli interessati

2. Scopo e ambito di applicazione

Scopo dell'Accordo è garantire il rispetto dell'art. 28 paragrafi 3 e 4 del Regolamento e definire le modalità attraverso le quali il Responsabile si impegna ad effettuare, per conto del Titolare, le operazioni di Trattamento dei Dati Personali svolte nel contesto dell'erogazione del Servizio *[indicare la tipologia del Servizio oggetto del contratto/convenzione/accordo principale in essere tra le parti]* e per effetto dell'adempimento del *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo]* in essere tra le Parti e come specificato nell'allegato 1.
Nel quadro della disciplina dettata dal Citato (*[indicare, ad esempio, se trattasi di contratto/convenzione/accordo]* le Parti hanno sottoscritto questo Accordo al fine di garantirsi reciprocamente il rispetto del Regolamento e delle leggi applicabili sulla protezione dei Dati Personali vigenti, stabilendo le tutele e le procedure necessarie affinché il trattamento avvenga nel rispetto delle suddette norme.
Il Titolare del trattamento ha preso atto che il Responsabile presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato.
Il Responsabile garantisce che la propria struttura ed organizzazione sono conformi alle normative vigenti necessarie l'esecuzione del presente Servizio e si impegna ad adeguarla ovvero a mantenerlo adeguato allo stesso, garantendo il pieno rispetto (per sé e per i propri collaboratori e dipendenti) delle presenti istruzioni oltre che di tutte le norme di legge in materia.
Gli allegati da 1 a 3 costituiscono parte integrante dell'Accordo.
Il presente accordo lascia impregiudicato gli obblighi cui è soggetto il Titolare del trattamento a norma del Regolamento. Il presente accordo non garantisce, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del Regolamento.

3. Definizioni

Ai fini del presente Accordo, i termini di seguito indicati, ove riportati con lettera iniziale maiuscola, avranno il seguente significato:

- **"Accordo"**: questo scritto;
- "**Altro Sub-Responsabile del trattamento" o "altro SUB-Responsabile":** (sia in forma singolare sia plurale) ogni ulteriore Responsabile del trattamento che venga eventualmente nominato dal Sub-Responsabile del trattamento sulla base dell'autorizzazione, specifica o generale, del Titolare e del Responsabile che si impegna a trattare i Dati Personali del Titolare, in adempimento degli obblighi del Responsabile Principale e del Titolare del trattamento ai sensi del presente Accordo;

- **“Autorità di vigilanza”**: qualsiasi autorità, incluso il Garante della protezione dei dati personali, che abbia il potere di monitorare e far rispettare l’osservanza del Regolamento e delle leggi applicabili sulla protezione dei Dati Personali del Servizio.
- **“Dati Personali”**: ai fini del presente Accordo, i Dati Personali sono i dati relativi ad **Interessati**, trattati in connessione con il Servizio fornito dal Responsabile del trattamento al Titolare e hanno il significato stabilito nel Regolamento, comprendendo, solo nei limiti in cui sono trattati dal Responsabile, anche le categorie di dati di cui agli artt. 9 e 10 del Regolamento.
- **“Diritti degli Interessati”**: i diritti cui sono destinatari gli Interessati ai sensi del Regolamento. A titolo esemplificativo e non esaustivo i Diritti degli Interessati includono il diritto di richiedere l'accesso, la rettifica o la cancellazione dei Dati Personali, di richiedere la limitazione del trattamento in relazione all'oggetto dei dati o di opporsi al trattamento, nonché il diritto alla portabilità dei dati;
- **“Interessato”:** (sia in forma singolare sia plurale) **persona fisica identificata o identificabile** alla quale si riferiscono i Dati Personali. Ai fini del presente Accordo, l’Interessato ha il significato stabilito nel Regolamento;
- **“Provvedimento”**: il provvedimento del 27 novembre 2008, comprensivo di successive modifiche, con il quale il Garante Privacy ha dettato misure ed accorgimenti per i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. In particolare, ai sensi del paragrafo d., del Provvedimento “nel caso di servizi di amministrazione di sistema affidati in outsourcing, il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema”. Provvedimento “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema” del 27 novembre 2008 così come modificato in base al provvedimento del 25 giugno 2009
- **“Regolamento”**: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali e sulla libera circolazione di tali dati;
- **“Responsabile” o “Responsabile del trattamento”:** in generale, una persona fisica o giuridica, autorità pubblica, agenzia o altro ente che tratta i Dati Personali per conto del Titolare;
- **“Responsabile della protezione dei dati”:** soggetto designato rispettivamente dal Titolare e/o dal Responsabile in conformità agli art. 37 e ss. del Regolamento;
- **“Servizio”**: il Servizio erogato dal Responsabile nei confronti del Titolare, come definito nel *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo]* in essere;
- “**Sub-Responsabile del trattamento”:** (sia in forma singolare sia plurale) ogni ulteriore Responsabile del trattamento che venga eventualmente nominato dal Responsabile Principale sulla base dell’autorizzazione, specifica o generale, del Titolare e che si impegna a trattare i Dati Personali del Titolare, in adempimento degli obblighi del Responsabile Principale ai sensi del presente Accordo;
- **“Titolare del trattamento” o “Titolare”:** in generale, la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o in collaborazione con altri, determina le finalità e i mezzi del trattamento dei Dati Personali;
- **“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;
- **“Violazione dei Dati Personali”**: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l’accesso non autorizzato a Dati Personali trasmessi, conservati o comunque trattati.

4. Dettagli sui Trattamenti effettuati dal Responsabile

Lo scopo, le categorie di dati personali e le finalità del Trattamento dei Dati Personali per le quali sono trattati per conto del Titolare nel contesto dell’erogazione del Servizio sono descritti nell'Allegato 1 al presente Accordo

5. Obblighi del Responsabile

Il Responsabile si impegna a procedere al Trattamento dei Dati Personali nel rispetto del Regolamento e delle leggi applicabili sulla protezione dei dati che, con la sottoscrizione del presente atto, dichiara di conoscere. In particolare s’impegna a:

- trattare i Dati Personali del Titolare solo se necessario a fornire il Servizio oggetto del *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo* e nel rispetto delle istruzioni scritte del Titolare, salvo che lo richieda il diritto dell’Unione o nazionale a cui è soggetto il Responsabile del trattamento. In tal caso il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. ile del trattamento informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Le istruzioni sono descritte nel presente Accordo. Il Titolare può impartire ulteriori istruzioni documentate successivamente per tutta la durata del trattamento dei dati;
- garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare del trattamento qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
- informare il Titolare nel caso in cui ritenga che specifiche istruzioni siano in violazione di leggi applicabili in materia di protezione dei dati;
- trattare i dati personali soltanto per le finalità specifiche del trattamento di cui Allegato 1, salvo ulteriori istruzioni fornite per iscritto dal Titolare del trattamento;
- rispondere prontamente ed adeguatamente alle richieste di informazioni del Titolare relative al trattamento dei dati conformemente al presente Accordo;
- notificare al Titolare senza ritardo qualsiasi contatto, comunicazione o corrispondenza che potrebbe ricevere da un'Autorità di vigilanza, in relazione al Trattamento dei Dati Personali degli Interessati;

- nel caso in cui il Responsabile nelle operazioni di Trattamento si avvalga di soggetti coinvolti nell'erogazione del Servizio, assicurerà che tali soggetti accedano solo ai dati personali del Titolare nella misura strettamente necessaria per l'attuazione, la gestione e il controllo previsto nell'Accordo:
  - siano stati debitamente designati per iscritto e abbiamo ricevuto le istruzioni previste per legge e impartite dal Responsabile in conformità con gli obblighi che lo stesso ha assunto per effetto del presente Accordo;
  - s'impegnino formalmente alla riservatezza o siano soggetti ad un obbligo legale di riservatezza vietando anche la divulgazione di informazioni, dati riservati senza autorizzazione del Titolare;
  - accedano con credenziali nominative e strettamente riservate solo ed esclusivamente ai dati necessari per l'erogazione del Servizio, sollevando il Titolare del trattamento da qualsiasi responsabilità per il loro operato e nella misura strettamente necessaria per l'attuazione, la gestione e il controllo previsto dal *(indicare, ad esempio, se trattasi di contratto/convenzione/accordo)*;
  - ricevano la formazione necessaria in materia di protezione dei Dati Personali;
- ove applicabile relativamente al Servizio fornito, procedere alla nomina di uno o più amministratori di sistema, individuati tenendo conto della loro esperienza professionale, in particolare con riferimento alle capacità ed affidabilità dimostrate nello svolgimento delle proprie mansioni, nelle forme e con le modalità indicate dall'Autorità di vigilanza ed eventualmente dal Titolare del trattamento, fornendo loro specifiche istruzioni e indicando espressamente i compiti attribuiti. Il Responsabile s'impegna a fornire al Titolare un elenco contenente i nominativi degli amministratori di sistema nominati e i rispettivi compiti attribuiti, provvedendo ad aggiornare l'elenco ogni qualvolta necessario (i.e. arrivo/cambio di mansione/cessazione). La nomina ad amministratore dovrà contenere quanto previsto dal Provvedimento e almeno le seguenti istruzioni:
  - rispettare le istruzioni impartite dal Titolare;
  - le credenziali di autenticazione, ivi incluso quelle che permettono l'accesso ai sistemi del Titolare, sono assolutamente personali e non cedibili, per nessuna ragione. Se si è in possesso di più credenziali di autenticazione, bisogna fare attenzione ad accedere ai dati unicamente con le credenziali relative al trattamento in oggetto. Le credenziali devono essere conservate in modalità sicura.
  - considerare i Dati Personali dei quali avrà conoscenza, nel corso dello svolgimento delle attività connesse all'incarico ricevuto, di titolarità del Titolare; pertanto dei tali dati non potrà esserne detenuta una copia se non espressamente autorizzati dal Titolare;
  - attenersi allo specifico e rigoroso divieto di comunicazione non autorizzata e di diffusione a qualunque titolo delle credenziali di accesso e dei Dati Personali eventualmente conosciuti;
  - collaborare con il Titolare mantenendolo informato della gestione e di eventuali anomalie che potrebbero compromettere la sicurezza dei dati;
  - informare il Titolare del trattamento in caso di mancato rispetto delle norme di sicurezza e in caso di eventuali incidenti;
- svolgere i controlli sull'operato degli amministratori di sistema designati, nonché sugli accessi logici ai sistemi di elaborazione e agli archivi elettronici effettuati dagli stessi amministratori di sistema, in conformità alle previsioni del Provvedimento comunicando il risultato di tali controlli al Titolare;
- vigilare affinché le persone autorizzate al trattamento e gli amministratori di sistema che operano sotto la propria direzione e/o autorità rispettino le istruzioni impartite e le misure tecniche e organizzative predisposte, segnalando al Titolare il mancato rispetto di dette istruzioni che potrebbero causare vulnerabilità ai dati trattati per conto di quest'ultimo;
- qualora previsto dalla tipologia di trattamento, prestare particolare attenzione al trattamento dei Dati Personali rientranti nelle categorie particolari o relativi a reati e condanne penali degli interessati conosciuti, anche incidentalmente, nel corso dell'erogazione del Servizio, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura. Il Responsabile applica limitazioni specifiche e/o garanzie supplementari per il trattamento di tale tipologia di dati personali;
- verificare la corretta osservanza, da parte delle persone autorizzate, delle misure previste dal Titolare in materia di archiviazione, potendo derivare gravi conseguenze da accessi non autorizzati alle informazioni oggetto di Trattamento da parte di coloro che operano nella propria struttura;
- collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei Dati Personali;
- vigilare affinché i Dati Personali degli interessati vengano comunicati solo a quei terzi necessari per lo svolgimento del Servizio e i Dati Personali non siano diffusi, salvo espressa autorizzazione del Titolare;
- dare immediato avviso al Titolare in caso di nuovi trattamenti e/o della cessazione di quelli concordati. Il Responsabile non deve creare banche dati nuove senza espressa autorizzazione del Titolare, fatto salvo quando ciò risulti strettamente indispensabile ai fini dell'esecuzione del Servizio;
- conservare la documentazione cartacea contenente Dati Personali nell'ufficio di destinazione originaria, avendo cura di non lasciarla esposta e/o facilmente accessibile, al fine di evitare accessi non autorizzati ai dati;
- utilizzare esclusivamente mezzi del trattamento dei Dati Personali adeguati alle normative vigenti, ivi compresi i provvedimenti delle competenti autorità, e volti (i) ad attuare in modo efficace i principi di protezione dei dati di cui alla normativa applicabile, ivi inclusi i principi della "privacy by design" e "privacy by default" e (ii) ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti della normativa applicabile e tutelare i Diritti degli Interessati;
- rispettare, in generale, tutte le disposizioni vigenti in materia di trattamento di Dati Personali, attuando gli eventuali provvedimenti giurisdizionali e/o amministrativi adottati dalla Autorità di vigilanza e ogni altra autorità all'uopo preposta;
- comunicare al Titolare del trattamento il nome ed i dati del proprio Responsabile della protezione dei dati, qualora ne abbia designato uno conformemente agli artt. 37 e ss. del Regolamento;
- tenere per iscritto un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare del trattamento ai sensi dell'art. 30 par. 2 del Regolamento;
- qualora previsto dal servizio erogato, garantire che i server, gli storage, le infrastrutture contenenti dati del Titolare e necessari per la loro gestione siano ubicati nel territorio Italiano o Europeo. Il Responsabile è obbligato ad avvisare il Titolare qualora tale condizione subisse modifiche. Se il Responsabile del trattamento, per l'erogazione del Servizio, fosse tenuto a procedere ad un

trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il Titolare del trattamento di quest'obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico.

6. Obblighi del Titolare

Il Titolare del trattamento s'impegna a:

- garantire che i dati conferiti al Responsabile siano esatti e aggiornati;
- garantire che i Trattamenti effettuati dal Responsabile per lo svolgimento del Servizio siano fondati su una delle condizioni di liceità del trattamento e, in generale, rispettino le condizioni previste dalla Normativa vigente in materia di protezione di dati personali;
- fornire e documentare le istruzioni relative al trattamento dei dati da parte del Responsabile, per garantire, prima e durante tutto il trattamento il rispetto degli obblighi previsti dal Regolamento;
- comunicare al Responsabile ogni eventuale modifica e rettifica dei Dati Personali, nonché qualsiasi richiesta da parte di un Interessato riguardante la cancellazione e/o la rettifica dei Dati Personali o la limitazione o opposizione al trattamento;
- fornire al Responsabile, su sua richiesta, le necessarie informazioni aggiornate per consentirgli la tenuta del registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento.

7. Diritti del Titolare

Il Titolare del trattamento ha il diritto di:

- vigilare sull'operato del Responsabile;
- aggiornare il presente Accordo e le istruzioni descritte nelle modalità che riterrà più opportune;
- richiedere al Responsabile contezza scritta della conformità al presente Accordo ed alle istruzioni scritte del Titolare;
- chiedere la cessazione e/o la sospensione del Trattamento qualora il Servizio, a seguito di verifiche successive, non dovesse essere conforme ai requisiti del Regolamento, oppure imposta dalla necessità di adempiere a divieti o obblighi derivanti dalla normativa sul trattamento dei Dati Personali o dalla Normativa Applicabile, e/o a provvedimenti dell'Autorità di Vigilanza o dall'Autorità Giudiziaria.

8. Autorizzazione alla designazione di Sub-Responsabili

Il Titolare riconosce e accetta che, per il solo scopo di erogare il Servizio e nel rispetto dei termini di cui al presente *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo]* e del Regolamento, il Responsabile del trattamento possa ricorrere ad altri Responsabili del trattamento (di seguito, "Sub-Responsabili"), nel caso in cui lo stesso, per il trattamento dei dati oggetto del Servizio, si avvalga di persone fisiche o giuridiche alle quali abbia eventualmente conferito il compito di svolgere attività e/o prestazioni riconducibili al Servizio.

Pertanto, il Titolare del trattamento fornisce al Responsabile un'autorizzazione generale a ricorrere a Sub-Responsabili, a condizione che il Responsabile:

- informi il Titolare in merito alla scelta, aggiunta cambiamento o sostituzione di qualsiasi Sub-Responsabile e riconosca al Titolare l'opportunità di valutarla, e se del caso opporvisi. Al fine di esercitare il proprio diritto ad opporsi al ricorso da parte del Responsabile a nuovi Sub-responsabili, il Titolare entro e non oltre quindici (15) giorni lavorativi informerà il Responsabile per iscritto della propria decisione. In caso di opposizione ad uno o più dei nuovi Sub-Responsabili spiegandone le ragioni. In tal caso, il Responsabile farà quanto in suo ragionevole potere per eventualmente rendere disponibile una diversa modalità di erogazione dei servizi oggetto del *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo]* in essere tra le Parti ai quali la nuova nomina a Sub-Responsabile afferisca;
- scelga diligentemente il Sub-responsabile, prestando particolare attenzione all'adeguatezza delle misure tecniche e organizzative adottate da quest'ultimo. Il Responsabile è tenuto a stipulare un accordo scritto con qualsiasi eventuale Sub-responsabile il quale deve (i) prevedere nei confronti del Sub-responsabile gli stessi obblighi previsti dal presente Accordo a carico del Responsabile, nella misura applicabile ai Servizi subappaltati, (ii) descrivere i Servizi subappaltati, (iii) le misure tecniche e organizzative che il Sub-responsabile è tenuto ad implementare e (iv) e le modalità di audit da parte del Responsabile del trattamento, del Titolare del trattamento o di soggetti terzi, laddove applicabili ai Servizi subappaltati (v) le misure necessarie per proteggere i segreti dell'Ente o altre informazioni riservate compresi i dati personali;
- se richiesto, trasmetterà al Titolare copia del contratto stipulato tra il Responsabile e il Sub-responsabile, omettendo dal medesimo qualsiasi informazione riservata che attenga esclusivamente il rapporto economico tra il Responsabile o il Sub-Responsabile o altri aspetti del rapporto rispetto al quale il Titolare è estraneo;
- verificare che i soggetti nominati Sub-responsabili rispettino e facciano rispettare le istruzioni, gli obblighi e le misure tecniche di sicurezza necessarie in relazione alle specifiche attività di trattamento poste in essere. Su richiesta scritta del Titolare, il Responsabile metterà a disposizione le informazioni necessarie per dimostrare il rispetto degli obblighi in capo a ciascun Sub Responsabile
- mantenga e notifichi al Titolare un elenco dei Sub-Responsabili designati e qualsiasi aggiornamento dello stesso;
- informi il Titolare del trattamento qualora il Sub-responsabile dovesse trasferire i dati in paesi Extra-UE. Solo previa autorizzazione del Titolare il Sub-responsabile potrà procedere a tale trasferimento.

Il Responsabile fornisce nell'Allegato 2 l'elenco dei Sub Responsabili già individuati alla data di sottoscrizione del presente Accordo

Spetta al Responsabile assicurare che ogni Sub-Responsabile presenti le stesse garanzie sufficienti alla messa in opera di misure tecniche ed organizzative appropriate, in modo che il trattamento risponda alle esigenze del Regolamento.

Il Responsabile che ricorre a Sub-Responsabili conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei Sub-Responsabili qualora questi omettano di adempiere ai propri obblighi in materia di protezione dei Dati Personali.

Il Responsabile notifica al Titolare del trattamento qualunque inadempimento, da parte del Sub-Responsabile del trattamento, degli obblighi contrattuali.

Il Responsabile del trattamento concorda con il Sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il Responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il Titolare del trattamento ha diritto di risolvere il contratto con il Sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

9. Diritti degli Interessati

Tenuto conto della natura del Trattamento, il Responsabile s'impegna ad assistere il Titolare consentendogli di adempiere agli obblighi che quest'ultimo ha di dar seguito alle richieste degli Interessati nell'esercizio dei diritti loro riconosciuti dal Regolamento, supportandolo, nella misura in cui ciò sia possibile, mediante misure tecniche e organizzative adeguate.

Qualora gli Interessati esercitino i diritti loro riconosciuti dal Regolamento presso il Responsabile del trattamento presentandogli la relativa richiesta, questi deve avvisare senza ritardo il Titolare inoltrando le istanze tramite i canali di contatto concordati con il Titolare (e-mail privacy@comune.baiso.re.it). Le Parti riconoscono e accettano che la responsabilità di rispondere a tali contatti, comunicazioni o corrispondenza è esclusivamente del Titolare e non del Responsabile.

10. Violazioni di Dati Personali

In caso di violazione dei dati personali trattati dal Titolare del trattamento, il Responsabile del trattamento coopera ed assiste il Titolare nell'ottenere le informazioni necessarie per permettere al Titolare l'eventuale notifica all'Autorità di vigilanza competente e ai soggetti interessati, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile.

Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal Titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:
a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679/, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2) le probabili conseguenze della violazione dei dati personali;
3)le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo

c) nell'adempiere, in conformità dell'articolo 34 del Regolamento all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento non oltre le 24 ore dopo esserne venuto a conoscenza al Responsabilee all'Ind mail privacy@comune.baiso.re.it.
Il Responsabile è consapevole che una violazione non è limitata ai soli accadimenti derivanti dall'esterno, ma include anche incidenti derivanti dal trattamento interno che violano i principi di sicurezza e riservatezza come definito all'art. 4 punto 12 del Regolamento. Il Responsabile ha l'obbligo della comunicazione della violazione al Titolare anche se le violazioni sono subite dall'eventuale Sub-responsabile. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
Le parti stabiliscono nell'allegato 3 tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del Regolamento.

Il Responsabile che viene a conoscenza di una Violazione dei Dati Personali dovrà adottare le appropriate misure di salvaguardia atte a contenerla e a mitigarne gli effetti.

11. Misure di sicurezza

Il Responsabile dichiara che il Servizio erogato è conforme ai requisiti del Regolamento e s'impegna ad adottare adeguate misure tecniche e organizzative ai sensi dell'articolo 32 del Regolamento, nonché ogni altra misura indicata dal Titolare, o comunque eventualmente indicata come adeguata dall'Autorità di vigilanza con propria circolare, risoluzione o qualsivoglia altro provvedimento eventualmente diversamente denominato, al fine di proteggere i Dati Personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzioni, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali).
Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

A titolo esemplificativo e non esaustivo il Titolare fornisce nell'allegato 3 un elenco delle misure tecniche e organizzative che il Responsabile deve avere adottato. Il Responsabile, inoltre, s'impegna ad adottare anche quanto previsto dal Provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e di svolgere i controlli sull'operato degli amministratori di sistema, nonché sugli accessi logici ai sistemi di elaborazione ed agli archivi elettronici effettuati da quest'ultimi, in conformità alle previsioni del Provvedimento comunicando il risultato di tali controlli al Titolare.
Il Responsabile si obbliga, infine, a monitorare il buon funzionamento dei sistemi e delle misure di sicurezza adottate, nonché il rispetto di queste da parte dei soggetti che trattano i Dati Personali impegnandosi ad aggiornare le misure di sicurezza implementate alla luce della tipologia dei Dati Personali e dei trattamenti che sono necessari per l'erogazione del Servizio nonché tenendo conto dello sviluppo delle prassi e della normativa in tema di misure di sicurezza

Il Responsabile comunica per iscritto le soluzioni e l'elenco delle misure individuate ed adottate per rispettare tali obblighi

12. Audit e verifiche

Il Responsabile s'impegna a mettere a disposizione del Titolare la documentazione e le informazioni necessarie per dimostrare il rispetto degli obblighi del presente Accordo, consentendo e contribuendo alle attività di revisione - comprese verifiche e ispezioni - realizzate dal Titolare o da un altro soggetto da questi incaricato.

Il Responsabile riconosce a accetta che il Titolare, in qualsiasi momento con un preavviso di almeno 15 giorni lavorativi, potrà chiedere al Responsabile la collaborazione per lo svolgimento, all'interno della struttura del Responsabile, di operazioni di verifica dell'esatto adempimento di quanto pattuito. L'attività di verifica potrà concretizzarsi sia attraverso attività di audit ed ispezione effettuate dal Titolare, direttamente o attraverso personale da questo incaricato, presso la sede del Responsabile del trattamento, sia attraverso la richiesta allo stesso di espletare attività di autovalutazione rispetto alle misure di sicurezza adottate ed all'osservanza delle misure impartite fornendone, a richiesta, documentazione per iscritto. In ogni caso il Titolare s'impegna affinché l'attività di verifica eventualmente svolta presso la sede del Responsabile del trattamento si svolga nel più breve tempo possibile – negli orari di ufficio e in giorni lavorativi – in modalità tale da non arrecare disturbo al regolare svolgimento dell'attività del Responsabile. I costi delle attività di audit saranno sostenute dal Titolare.

Il Responsabile, laddove proceda alla designazione di Sub-responsabili, si impegna a svolgere, a nome e per conto del Titolare, le attività di controllo di cui al capoverso precedente nei confronti di tali ultimi Sub-responsabili e, comunque, si obbliga ad impegnare questi ultimi a consentire i controlli del Titolare.
Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui al presente articolo, compresi i risultati di eventuali attività di revisione.

13. Trasferimenti internazionali

Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile del trattamento è effettuato soltanto su istruzione documentata e scritta del Titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

Il Titolare del trattamento conviene che, qualora il Responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il Responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte

14. Valutazione d'impatto

Il Responsabile, tenendo conto della natura del trattamento e per quanto di propria competenza, assiste il Titolare nella realizzazione della valutazione d'impatto relativa alla protezione dei dati e nella consultazione preventiva all'Autorità di Vigilanza, conformemente agli artt. 35 e 36 del Regolamento.

Il Responsabile ha l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche e ha l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

15. Inosservanza *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo* **e risoluzione**

Fatte salve le disposizioni del Regolamento Europeo 2016/679, qualora il Responsabile violi gli obblighi che gli incombono a norma del presente accordo, il Titolare può dare istruzione al Responsabile di sospendere il trattamento dei dati personali se quest'ultimo non rispetta il presente Accordo. Il Responsabile informa prontamente il Titolare qualora, per qualunque motivo, non sia in grado di rispettare il presente accordo.

Il Titolare ha il diritto di risolvere il contratto nei seguenti casi:

a) il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare in conformità del punto precedente e il rispetto del presente Accordo non sia ripristinato entro un termine ragionevole;
b) il Responsabile violi in modo sostanziale o persistente il presente Accordo, le decisioni vincolanti di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi al presente Accordo o gli obblighi che gli incombono a norma del Regolamento Europeo 2016/679.

Il Responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma del presente Accordo qualora, dopo aver informato il Titolare che le sue istruzioni violano i requisiti giuridici applicabili, il Titolare del trattamento insista sul rispetto.

16. Responsabilità

Qualora dall'inottemperanza degli obblighi previsti dal presente Accordo o dal Regolamento in capo al Responsabile dovesse derivare al Titolare l'applicazione di una sanzione, ivi inclusa una sanzione amministrativa pecuniaria, o qualsivoglia pregiudizio, costo o spesa, il Responsabile sarà ritenuto direttamente responsabile nei confronti del Titolare, obbligandosi sin da ora a manlevare e tenere indenne il Titolare.

Il Responsabile si impegna a manlevare e tenere indenne il Titolare da ogni eventuale danno, spesa, costo o onere derivanti da una Violazione dei Dati Personali subita dal Responsabile o da qualsivoglia Sub-responsabile.

17. Modifiche della Normativa vigente in materia di protezione dei dati personali

Nel caso in cui intervengano modifiche della Normativa vigente in materia di protezione dei dati personali per in grado di incidere sulle responsabilità e gli obblighi imposti dal presente Accordo, il Titolare può proporre le modifiche del presente Accordo necessarie al rispetto delle nuove previsioni normative.

Le modifiche si intendono approvate dal Responsabile se questi non si oppone entro 7 giorni lavorativi dalla ricezione delle stesse.

Ove l'Accordo sia modificato, il Responsabile del trattamento s'impegna affinché variazioni equivalenti siano apportate, senza ritardo, negli accordi posti in essere con i Sub-Responsabili

Nel caso in cui il Responsabile non accetti le modifiche dovrà fornire idonea motivazione, e il Titolare e il Responsabile si impegnano a discutere e negoziare in buona fede le possibili modifiche al presente Accordo necessarie al rispetto della Normativa vigente in materia di protezione dei dati personali.

Qualora non venga trovato un accordo durante le negoziazioni del presente Accordo o qualora il Responsabile non motivi il rifiuto delle modifiche proposte dal Titolare, il Titolare avrà facoltà di recedere dal contratto/ordine di acquisto e dal presente Accordo, con conseguente applicazione dell'articolo 16 del presente Accordo.

18. Cooperazione con l'Autorità di vigilanza

Il Responsabile si obbliga ad informare il Titolare, senza ritardo e per iscritto, in merito ad ispezioni ricevute da parte dell'Autorità di vigilanza o dell'Autorità Giudiziaria aventi ad oggetto questioni rilevanti in materia di protezione dei Dati Personali.

Il Responsabile si impegna altresì a collaborare, su richiesta del Titolare, in qualunque indagine svolta dalle autorità indicate in precedenza e/o qualsiasi altra autorità pubblica italiana o estera.

19. Restituzione e cancellazione dei dati.

Alla cessazione dell'erogazione del Servizio il Responsabile del trattamento, senza alcun costo per il Titolare e senza indebito ritardo, è tenuto a cancellare o, a scelta del Titolare, a restituirgli tutti i Dati Personali, qualora conservati sui sistemi del Responsabile. In caso di cancellazione il Responsabile dovrà adottare sistemi che permettano una cancellazione sicura di tutte le

copie esistenti, ivi incluso i back up, entro 90 giorni, certificando e documentando per iscritto l'esecuzione di tali adempimenti, salvo che obblighi di legge impediscano tale cancellazione. Finché i dati non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.
All'atto della restituzione e/o cancellazione dei dati il Responsabile dovrà fare rispettare le stesse Istruzioni anche al/ai Sub-Responsabile/i (qualora designato/i).

20. Validità, cessazione e modifiche

Il presente Accordo è da ritenersi valido per tutta la durata dell'erogazione del Servizio da parte del Responsabile, così come stabilite nel *[indicare, ad esempio, se trattasi di contratto/convenzione/accordo]* in essere tra le Parti e delle operazioni di trattamento ad esso connesse.

Le parti possono proporre eventuali modifiche all'Accordo, ove le ritengano ragionevolmente necessario anche per soddisfare i requisiti delle leggi applicabili alla protezione dei Dati Personali.

Ove l'Accordo sia modificato, il Responsabile del trattamento s'impegna affinché variazioni equivalenti siano apportate, senza ritardo, negli accordi posti in essere con i Sub-Responsabili.

Luogo e data

Per *[indicare denominazione Ente]*
[indicare riferimenti soggetto sottoscrittore]

Per il Responsabile, per integrale accettazione dell'Accordo:
[indicare riferimenti soggetto sottoscrittore]

Allegato 1: dettagli sui trattamenti effettuati dal Responsabile

Il presente Allegato include alcuni dettagli sul Trattamento dei Dati Personali che il Responsabile è autorizzato ad effettuare per conto del Titolare, come richiesto dall'articolo 28, par. 3, del Regolamento.

CATEGORIE DI DATI PERSONALI

I Dati Personali oggetto di trattamento si riferiscono alle seguenti categorie di dati:

- ☐ dati di contatto (nome e cognome, indirizzo e-mail, indirizzo postale, numero di telefono)
- ☐ data di nascita
- ☐ età
- ☐ sesso
- ☐ altro (si prega di specificare):

_____

_____

_____

CATEGORIE PARTICOLARI DI DATI PERSONALI (OVE PRESENTI)

I Dati Personali oggetto di trattamento si riferiscono alle seguenti Categorie Particolari di Dati Personali:

- ☐ disabilità e/o infortuni
- ☐ orientamento politico
- ☐ convinzioni etniche o religiose
- ☐ orientamento sessuale in cui è implicita la relazione o lo stato coniugale
- ☐ appartenenza sindacale
- ☐ stato di salute e/o malattie
- ☐ reati o condanne penali
- ☐ altro (si prega di specificare):

_____

_____

_____

INTERESSATI

I dati personali oggetto di trattamento riguardano le seguenti categorie di interessati:

- ☐ candidati da considerare per l'instaurazione di un rapporto di lavoro
- ☐ servizi del settore finanze, bilancio e Controllo di gestione
- ☐ servizi dell'ufficio ambiente
- ☐ servizi erogati dall'URP
- ☐ servizi sociali
- ☐ patrimonio immobiliare
- ☐ Servizio di biblioteca
- ☐ Servizio sport
- ☐ settore Cultura
- ☐ anagrafe degli animali da affezione (A.R.A.A.)
- ☐ attività dei lavori pubblici
- ☐ attività del patrimonio immobiliare, artistico e storico
- ☐ attività dei tributi
- ☐ attività del commercio
- ☐ attività delle onoranze funebri
- ☐ attività della polizia municipale
- ☐ attività dell'urbanistica
- ☐ attività di comunicazione
- ☐ attività gabinetto del Sindaco
- ☐ attività culturali e/o sportive
- ☐ sportello unico edilizia
- ☐ lavoratori in somministrazione
- ☐ personale dipendente e personale parasubordinato

Commento [CC1]: Selezionare i soggetti interessati e verifica in privacylab

☐ servizi demografici
☐ stagisti e/o tirocinanti
☐ SUAP
☐ altro (si prega di specificare): _____

_____

_____

_____

Commento [CC2]: Inserire parte di privacylab

NATURA DEL TRATTAMENTO: *(SPECIFICARE SE SI TRATTA DI TRATTAMENTO CON UTILIZZO DI DOCUMENTI CARTACEI, INFORMATIZZATI, IN CLOUD BACK UP, ECC)*

FINALITA' DEL TRATTAMENTO PER LE QUALI I DATI PERSONALI SONO TRATTATI PER CONTO DEL TITOLARE:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

DURATA DEL TRATTAMENTO: erogazione del servizio oggetto del presente Accordo erogato per conto del Titolare

Allegato 2
(da compilare da parte del Responsabile)

Elenco dei Sub Responsabili già individuati alla data della stipula dell'accordo

Cognome Nome / Ragione Sociale ed indirizzo	Nome, qualifica e dati di contatto del referente,	Partita Iva	Descrizione, tipologia e natura del Servizio erogato	Nazione di conservazione dei dati	Tempo di conservazione dei dati

Allegato 3: Istruzioni aggiuntive

Qualora il Responsabile conservi sui propri sistemi dati del Titolare, oppure acceda a sistemi che contengono dati del Titolare, oppure sia previsto dal rapporto contrattuale in essere, il Responsabile del trattamento mette in atto almeno le misure tecniche e organizzative qui di seguito specificate, per garantire la sicurezza dei dati personali come previsto dall'art. 32 del GDPR e dalla normativa vigente in materia di trattamento di dati personali

Il Responsabile garantisce:

a. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e, ove previsto dal Servizio erogato, la resilienza dei sistemi così da assicurare sempre la disponibilità dei Servizi che vengono forniti e la adeguata protezione dei dati che sono trattati con tali sistemi/servizi di trattamento;

b. di proteggere le reti informatiche da sistemi di sicurezza perimetrale (c.d. Firewall) e da altre apparecchiature appositamente predisposte allo scopo e mantenute aggiornate allo stato dell'arte.
Ogni postazione di lavoro del Responsabile deve essere protetta da sistemi di sicurezza contro le minacce informatiche (antivirus) e ne deve essere consentito l'utilizzo unicamente mediante appositi sistemi di autenticazione e profilazione;

c. di avere adottato una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

d. di avere adottato le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" stabilite da AGID con la circolare del 18 aprile 2017, n. 2/2017 pubblicata sulla Gazzetta Ufficiale. L'elenco delle misure è descritto all'indirizzo: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Di seguito si riporta in modo esemplificativo e non esaustivo la descrizione delle misure tecniche e organizzative di sicurezza per il trattamento dei dati oggetto del presente Accordo che costituiscono ulteriore specifica di quanto indicato in quest'ultimo.

GESTIONE DEGLI ACCESSI
Per una corretta gestione degli accessi è necessario che il Responsabile implementi misure sia di natura informatica, sia organizzativa. Lo scopo di tale gestione deve garantire l'accesso ai dati personali solo agli utenti interni ed esterni del Responsabile nella misura strettamente necessaria per lo svolgimento delle proprie mansioni lavorative.

- **Autenticazione degli utenti**
  Ciascun utente di un determinato sistema deve essere dotato di un proprio account nominale ed individuale. Questo adempimento è necessario al fine di potere verificare univocamente l'identità dell'utente, riconducendo a lui con certezza le azioni compiute all'interno del sistema, al fine di facilitare il rispetto del principio di accountability.
  La connessione fra autenticazione e accountability è stata sottolineata dal Garante per la protezione dei dati personali nel provvedimento 9101974 del 4/4/2019: "*l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresenta una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate*".

  Tale adempimento è inoltre incluso negli standard di sicurezza pubblicati dalle organizzazioni internazionali più prestigiose, e non richiede alcun costo aggiuntivo. Il Responsabile del trattamento deve implementare adeguate policy e procedure tali da garantire la corretta identificazione degli utenti e degli amministratori che accedono ai sistemi che gestiscono i Dati Personali del Titolare.

  In caso di **accesso dall'esterno**, ogni utente deve essere autenticato in modo corretto attraverso meccanismi di autenticazione sicuri (es.: password, smart card, certificati digitali, tecniche biometriche, ecc…)
  Tali meccanismi di autenticazione devono essere oggetto di specifiche politiche di generazione, utilizzo, custodia, aggiornamento e distruzione.

  Il Responsabile del trattamento deve identificare il/i custode/i delle password di sistema.

  Si ricorda che l'accesso di terzi non autorizzati a dati personali contenuti in aree riservate, costituisce una violazione grave della sicurezza in quanto sfruttabile da qualunque persona.
  Il Responsabile deve impartire precise istruzioni agli autorizzati al trattamento affinché adottino le necessarie cautele per assicurare la segretezza delle loro credenziali e la sicurezza dei dispositivi necessari per l'autenticazione.
  Occorre inoltre prevedere apposite procedure per la sostituzione degli autorizzati in caso di prolungata assenza o impedimento, al fine di assicurare la disponibilità dei trattamenti di dati.

  I diritti di accesso ai Dati Personali delle persone autorizzate sono rivisti a intervalli regolari, secondo il corretto processo di Identity and Access Management del Responsabile.

- **Autorizzazione degli utenti**
  Oltre agli account individuali il Responsabile deve definire le categorie di dati accessibili da ogni singolo account in funzione delle autorizzazioni assegnate (attività di profilazione degli accessi).
  La necessità di prevedere autorizzazioni specifiche (quantomeno interne ad un'organizzazione) emerge implicitamente anche dall'articolo 29 GDPR, ai sensi del quale "chiunque agisca sotto l'autorità del titolare o del responsabile, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso…". In caso di mancata profilazione dei soggetti autorizzati si configura una violazione ai sensi dell'art. 32 del GDPR e la mancata implementazione di sistemi di autorizzazione comporta la violazione dell'articolo 5 comma 1 lett. f del GDPR.

L'autorizzazione all'accesso ai dati può essere impostata anche sulla base dell'appartenenza di un utente ad un determinato gruppo. I profili di autorizzazione del gruppo devono definire in dettaglio i trattamenti e le azioni consentite.
Al momento dell'assunzione il Responsabile deve prevedere una procedura che gestisca il diritto di accesso ed il relativo profilo dei nuovi assunti in base al proprio ruolo. I profili devono essere verificati periodicamente, e comunque almeno una volta l'anno.

CONSERVAZIONE E CONDIVISIONE DEI DATI
Il GDPR obbliga l'adozione di misure tecniche ed organizzative e di procedure adeguate per garantire la minimizzazione dei dati. *I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento.*

Nell'ambito della sicurezza informatica evidenziamo i seguenti casi: :
- utilizzo nelle attività quotidiane;
- trasmissione a terzi;
- archiviazione.

- **La protezione dei dati trattati utilizzati nelle attività quotidiane**
  I dati utilizzati per le attività quotidiane devono essere in chiaro e non possano essere né pseudonimizzati, né cifrati. Le misure di sicurezza adottate dal Responsabile devono garantire la sicurezza dei dati trasmessi o archiviati.

- **La protezione dei dati trasmessi a terzi**
  Il dato trasmesso a terzi può essere intercettato e pertanto il dato condiviso può subire una violazione di confidenzialità.
  Per questo il Responsabile non deve utilizzare servizi che non prevedono la cifratura sicura dei dati, come ad esempio il protocollo http, che non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità della fonte.
  Il Responsabile deve pertanto crittografare (cryptography in transit) tutti i Dati Personali che transitano all'interno e all'esterno della rete del Responsabile attraverso i protocolli standard la cui sicurezza è assicurata. Il mancato utilizzo di strumenti di crittografia per la trasmissione dei dati si pone in contrasto con quanto previsto dall'articolo 32 del GDPR. La crittografia si applica, ovviamente, anche alle email. L'utilizzo di protocolli di cifratura, come il protocollo TLS e la cifratura end-to-end delle email in trasmissione costituisce, quindi, una misura di sicurezza adeguata ai sensi dell'articolo 32 del GDPR.

- **La protezione dei dati archiviati**
  Il Responsabile deve provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto a quanto previsto dal presente Accordo e deve adeguatamente proteggerli.
  Il Responsabile deve implementare una data retention policy per eliminare i dati non più necessari. Il periodo di conservazione dei Dati Personali deve essere specifico per ogni singola attività di trattamento, nel rispetto degli obblighi legali e/o regolamentari vigenti.

  Il personale del Responsabile non deve archiviare dati su supporti digitali portatili, salvo che quest'ultimi presentino le adeguate misure di sicurezza, ivi incluso la cifratura del supporto. L'assenza della cifratura dell'hard disk del dispositivo portatile che contiene dati personali costituisce una vulnerabilità e la sua assenza può essere sanzionata. Si precisa che in caso di archiviazione di dati su supporti digitali portatili del Responsabile, i dati devono essere conservati anche sui sistemi di archiviazione del Responsabile.
  I dati personali di natura particolare (Art. 9 del GDPR) o relativi a reati e condanne penali (Art. 10 del GDPR) archiviati devono essere cifrati o pseudoanominizzati.

  Il Responsabile deve avere adottato una procedura per la dismissione degli asset e dei supporti informatici e deve avere messo in atto procedure di pulizia sicura al fine di rimuovere in via definitiva e certificata tutti i Dati Personali e/o sovrascriverli in modo sicuro prima dello smaltimento o del riutilizzo.

  Oltre ai controlli di sicurezza informatica occorrerà prevedere anche controlli amministrativi e fisici, come ad esempio, proteggere adeguatamente i supporti dove sono fisicamente contenuti i dati del Titolare attraverso la chiusura a chiave e il registro degli accessi fisici al luogo di conservazione del supporto.

  Supporti cartacei:
  Relativamente ai supporti cartacei, si ricorda la necessità di adottare i seguenti i criteri di protezione dei dati:
  1. Qualsiasi documento in entrata/uscita appartenente a soggetti interessati del Titolare deve essere inserito in apposite cartelline non trasparenti, raccoglitori o buste;
  2. Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo devono essere richiuse dopo la consultazione in armadi o cassettiere, che dopo l'orario di lavoro saranno chiuse a chiave;
  3. Le copie cartacee delle e-mail inviate e ricevute dovranno essere archiviate in appositi raccoglitori che successivamente verranno archiviati in armadi;
  4. Tutti gli archivi cartacei devono essere chiusi all'interno di raccoglitori inseriti in armadi chiusi.

PROTEZIONE DEI DATI E DEI SISTEMI
I dati e i sistemi elettronici devono essere protetti da accessi non consentiti. Il Responsabile deve utilizzare software che permettono il contrasto ai virus e ai malware informatici e devono essere aggiornati periodicamente.
Anche i sistemi operativi e gli applicativi utilizzati per il trattamento dei dati devono essere aggiornati periodicamente.
I soggetti autorizzati devono essere formati al fine di minimizzare il rischio di un utilizzo improprio degli strumenti elettronici.

PROCEDURE DI BACK UP
I dati e i sistemi devono essere protetti da incidenti o violazione dei dati tramite un sistema di backup dei dati almeno giornaliero.

Qualora il Servizio preveda che i dati personali forniti dal Titolare siano contenuti e conservati nei sistemi del Responsabile, questi dovranno essere utilizzati solo ed esclusivamente al fine di eseguire le attività inerenti al Servizio. Copia di tali dati può essere fatta solo a fini esclusivi di back–up, ed è espressamente vietato qualsiasi altro utilizzo, comunicazione, copia (parziale o totale) dei dati stessi senza il preventivo consenso scritto del Titolare.

Il Responsabile deve predisporre e verificare una procedura scritta di ripristino dei back up. Il Responsabile del trattamento deve mettere in atto adeguate procedure per ripristinare la disponibilità dei Dati Personali del Titolare conservati presso il Responsabile in modo tempestivo e continuo. Le procedure di backup devono garantire una conservazione delle copie di backup almeno settimanale e devono prevedere il salvataggio off-line di una retention dei dati non inferiore a 15 gg/1mese per garantire da distruzioni dovute ad attacchi hacker e ransomware.
Il personale autorizzato al back up deve essere identificato per garantire la continuità del Servizio al Titolare.

NETWORK E SISTEMI DI SICUREZZA
Il Responsabile deve prevedere l'utilizzo di sistemi di monitoraggio sul perimetro della propria rete che analizzano il traffico dell'Ente al fine di controllare il flusso dei dati dall'interno verso l'esterno e dall'esterno verso l'interno.
Il Responsabile deve configurare il firewall/router al fine di limitare il traffico, in entrata e in uscita, da reti "non attendibili" (inclusi wireless).
Deve altresì essere negato tutto il resto del traffico ad eccezione dei protocolli necessari all'ambiente che tratta Dati Personali anche del Responsabile. In alternativa è possibile utilizzare firewall evoluti che permettono di predire il traffico e gestirlo tramite sistemi di intelligenza artificiale.
I firewall devono essere configurati al fine di proteggere, verificare e convalidare il traffico che è diretto ai sistemi. Qualsiasi Servizio o traffico non autorizzato deve essere bloccato.

IMPOSTAZIONE DEI LOG DEI SISTEMI
La conservazione e l'analisi dei messaggi di log costituisce una misura di sicurezza essenziale in quanto non solo permette al Titolare di essere sempre a conoscenza degli eventi che si verificano nei propri sistemi (ad esempio, accessi o operazioni compiute dagli utenti), ma soprattutto di essere sempre in grado di dimostrare l'adeguatezza delle misure di sicurezza implementate.
Si ricorda che la registrazione e la conservazione dei log è espressamente richiesta in diversi provvedimenti settoriali emanati dalle autorità di controllo.
In assenza di log non è possibile individuare vulnerabilità, né per quanto riguarda il Titolare, né per quanto riguarda le autorità di controllo. Inoltre, in assenza di log, non è possibile analizzare ex post le modalità di un attacco e, soprattutto, le conseguenze con riguardo ai dati personali conservati.
Il Responsabile deve altresì attivare sistemi di monitoraggio che devono registrare almeno le seguenti voci nel registro dei log:
- Identificazione dell'utente
- Tipo di evento
- Data e ora
- Fonte dell'evento
- Identità dei dati interessati (qualora il sistema lo permetta)

Il Titolare del trattamento dei Dati Personali ha il diritto di ottenere i log dai Responsabili del trattamento e/o dai Sub-responsabili.

CODICI DI CONDOTTA E CERTIFICAZIONI
Il Responsabile del trattamento aderisce ai codici di condotta e certificazioni qualora pubblicate dal Comitato.
I codici di condotta è le certificazioni non esimono, però, i Titolari da eventuali responsabilità.

ORGANIZZAZIONE E FORMAZIONE DELLE PERSONE
È necessario che il Responsabile attui un programma formale di sensibilizzazione sulla sicurezza per rendere consapevole tutto il personale delle politiche e delle procedure relative alla sicurezza dei Dati Personali.
Per questo il Responsabile deve:

- istruire e formare il proprio personale sulle corrette regole di condotta da adottare per la protezione dei Dati Personali accessibili dai sistemi del Responsabile (ad es: accesso mediante credenziali riservate, implementazione di screen saver con password che si attivano dopo un breve periodo di inattività ecc...).
- istruire e formare il proprio personale sulle corrette regole di condotta da adottare per il trattamento dei Dati Personali contenuti nei documenti cartacei (ad es: in caso di allontanamento dalla postazione di lavoro assicurarsi che nessuno possa accedere alle informazioni riservate proteggendo i documenti originali e le fotocopie da furto o uso non autorizzato, conservando la documentazione in cassetti e armadi chiusi alla fine della sessione di lavoro).

Le responsabilità e i doveri degli autorizzati relative alla riservatezza dei Dati Personali devono essere validi anche dopo la cessazione o il cambio di impiego.

Il Responsabile deve avere in essere chiari accordi contrattuali con i fornitori dei servizi (Sub-responsabili), al fine di pattuire la loro responsabilità in merito alla sicurezza dei Dati Personali che trattano/memorizzano/trasmettono per conto del Titolare.

VIOLAZIONE DEI DATI PERSONALI

I processi e gli strumenti per la gestione degli incidenti devono essere correttamente implementati e/o migliorati al fine di consentire il rilevamento e la classificazione delle violazioni dei Dati Personali in modo che siano correttamente comunicati al Titolare affinché possa provvedere entro i termini stabiliti alla gestione della violazione (vedi anche punto 10).
Il Responsabile ha l'obbligo di creare e mantenere aggiornato uno specifico registro delle violazioni dei Dati Personali.

MISURE DI AUDITING
Al Responsabile è richiesto di verificare periodicamente la sicurezza dei suoi sistemi attraverso:

- **Vulnerability scan**
  Strumento imprescindibile per le organizzazioni complesse o per quelle che hanno server accessibili da Internet e che, pertanto, espongono dati al pubblico. Secondo l'ICO e il Garante per la protezione dei dati personali i vulnerability scan dovrebbero essere effettuati regolarmente, e comunque a seguito di cambiamenti importanti.

- **Penetration test**
  Strumento essenziale di ogni Sistema di Gestione della Sicurezza delle Informazioni, poiché identifica le debolezze e le vulnerabilità che possono essere sfruttate dagli hacker.

Commento [c3]: Valutare a seconda dei casi