Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 PARAGRAFO 3) DEL REGOLAMENTO UE N. 2016/679

Tra

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE, (P. IVA: 09323530965), in persona del suo legale rappresentante pro tempore, con sede legale in Garbagnate Milanese (MI), viale Forlanini, 95, in qualità di Titolare del trattamento ex artt. 4 n. 7) e 24 del Regolamento UE n. 2016/679 (GDPR) (infra "ASST RHODENSE" e/o "Titolare del trattamento");

e

……, (C. f. e P. IVA: ……), in persona del suo legale rappresentante pro tempore, con sede legale in ……, via ……, ……, in qualità di Responsabile del trattamento ex artt. 4 n. 8) e 28 del GDPR (infra "Responsabile del trattamento" e/o "Fornitore").

Il Titolare ed il Responsabile potranno essere denominati, di seguito, congiuntamente anche come le "Parti".

1. Premesse.

1.1. Le Parti hanno concordemente convenuto, ai sensi dell'art. 28 paragrafo 3) del GDPR, le seguenti clausole contrattuali (infra "Clausole"/"Contratto di nomina" e/o "Contratto") volte a disciplinare la nomina del Fornitore quale Responsabile del trattamento, ad opera di ASST RHODENSE, nella sua veste di Titolare del trattamento, a fronte dello svolgimento, da parte di quest'ultima, di un processo preventivo di risk assessment[1] volto a valutare e documentare, in un'ottica di accountability ex art. 5 paragrafo 2) del GDPR (e di culpa in eligendo), il grado di affidabilità e di capacità, in capo al Responsabile del trattamento qui nominato, di fornire le garanzie necessarie, idonee ed adeguate a rendere, mediante l'adozione di misure di sicurezza tecniche ed organizzative ex art. 32 del GDPR, conforme il trattamento di specie alla normativa comunitaria e nazionale sulla protezione dei dati personali, ivi incluse le pronunzie e gli atti di cd. soft law emessi sul tema: a tal riguardo, giova precisare che l'onere previsto dall'art. 28 paragrafo 1) e Considerando n. 81) del GDPR è di natura continua, e, dunque, non termina nel momento in cui il Titolare ed il Responsabile del trattamento concludono un contratto o atto giuridico, dato che il primo è tenuto a verificare, ad intervalli appropriati, che il nominato Responsabile del trattamento possegga, in modo costante, le garanzie richieste, anche grazie all'esecuzione di appositi audit o ispezioni, ove appropriato e necessario.

1.2. Nel contesto del contratto sottoscritto tra le Parti in data …… di cui al provvedimento n. ……. del ……., il Responsabile del trattamento provvede a svolgere, per conto del Titolare, le operazioni di trattamento meglio descritte nell'allegato 1) del presente Contratto di nomina (il quale, assieme ai restanti allegati, costituisce parte integrante del Contratto di nomina medesima), in conformità al Contratto di nomina ed alla normativa comunitaria e nazionale sulla protezione dei dati personali, ivi inclusa la relativa giurisprudenza, dottrina dominante ovvero normativa di secondo livello (soft law).

2. Obblighi del Responsabile del trattamento.

2.1. Fatti salvi gli altri obblighi previsti dalle disposizioni di legge applicabili, ivi inclusi gli atti di soft law ovvero i Provvedimenti ad opera delle competenti Autorità di controllo ovvero di natura giurisdizionale, il Responsabile del trattamento è obbligato a svolgere i seguenti compiti:

a. Trattare i dati personali sulla base del presente Contratto di nomina, sulla base del contratto descritto al precedente punto 1.2) ovvero in ragione di ogni altra istruzione impartita formalmente dal Titolare del trattamento, anche in caso di trasferimento dei relativi dati personali verso un paese terzo (ossia, situato al di fuori del Spazio Economico Europeo (SEE)) o un'organizzazione internazionale, salvo che lo richieda il diritto dell'UE o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento è tenuto ad informare il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

[1] Tale attività di risk assessment viene svolta, in via generale, mediante l'analisi e scambio di una serie di documenti (es. informative ex artt. 13 e 14 del GDPR; termini di servizio; registro delle attività del trattamento ex art. 30 del GDPR; valutazione d'impatto sulla protezione dei dati ex art. 35 del GDPR; policy circa la sicurezza tecnica delle informazioni; certificazioni ottenute; rapporti di soggetti terzi; audit di terze parti). La valutazione, da parte del Titolare del trattamento, circa la sufficienza delle garanzie del Responsabile del trattamento è definibile, in sostanza, come una forma di valutazione del rischio, dipesa, in larga misura, dalla tipologia di trattamento affidato al Responsabile, da valutarsi caso per caso, tenendo conto della natura, portata, contesto e finalità del trattamento, così come i rischi per i diritti e le libertà delle persone fisiche.
I seguenti elementi devono essere, in teoria, presi in considerazione dal Titolare del trattamento, al fine di valutare la sufficienza delle garanzie offerte dal Responsabile del trattamento: competenza settoriale e/o tecnica; affidabilità; risorse; reputazione sul mercato; certificazione; codici di condotta, anche di natura settoriale.

b. Garantire che le proprie persone autorizzate al trattamento ex artt. 4 n. 10), 29 e 32 n. 4) del GDPR – previamente designate per iscritto, e adeguatamente istruite circa l'ambito di attività di trattamento oggetto di tale autorizzazione – si siano impegnate alla riservatezza ovvero abbiano un adeguato obbligo legale di riservatezza[2];
c. Adottare le misure di sicurezza tecniche ed organizzative richieste dall'art. 32 del GDPR (meglio illustrate, seppur in via generale, al relativo allegato 3)), tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come anche il rischio di (varia) probabilità e gravità per i diritti e le libertà delle persone fisiche, onde così assicurare un livello di sicurezza adeguato al rischio associato alle attività di trattamento demandate;
d. Rispettare le condizioni di cui all'art. 28 paragrafo 2) del GDPR, al fine di ricorrere ad un altro (sub) Responsabile del trattamento, così declinate nel caso di specie: il Responsabile del trattamento ha l'autorizzazione generale del Titolare del trattamento per l'assunzione di (sub) Responsabili del trattamento[3]; l'elenco dei (sub) Responsabili del trattamento già autorizzati dal Titolare del trattamento, al momento della sottoscrizione del presente atto, è contenuto nell'allegato 2).
e. Rispettare le condizioni di cui all'art. 28 paragrafo 4) del GDPR, laddove il Responsabile del trattamento si avvale di un (sub) Responsabile del trattamento per lo svolgimento di specifiche attività di trattamento: a tal riguardo, il Titolare del trattamento ha la facoltà di domandare al Responsabile del trattamento di fornirgli copia del contratto (o atto giuridico) sottoscritto tra quest'ultimo e il relativo (sub) Responsabile del trattamento nominato;
f. Tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, per quanto possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti del soggetto interessato di cui al capo III) del GDPR;
g. Assistere il Titolare del trattamento nel garantire il rispetto degli adempimenti in materia di misure di sicurezza tecniche ed organizzative di cui all'art. 32 del GDPR, così come individuate, di volta in volta, dal Titolare del trattamento, ivi incluse le seguenti: i) pseudonomizzazione e/o cifratura dei dati personali; ii) capacità di assicurare la riservatezza, l'integrità e la disponibilità dei dati e la resilienza dei sistemi e dei servizi di trattamento; iii) capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; iv) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
h. Assistere il Titolare del trattamento nell'esecuzione dell'onere di notifica e/o di comunicazione, ai sensi degli artt. 33 e 34 del GDPR, di una violazione di dati personali (data breach) ex art. 4 n. 12) del GDPR riferita ad un attività di trattamento svolta dal Responsabile del trattamento ovvero dal nominato (sub) Responsabile del trattamento: a tal fine, il Responsabile del trattamento è tenuto ad informare il Titolare del trattamento di tale evento immediatamente o, comunque, entro il termine (inderogabile) di n. 24 (ventiquattro) ore dal momento in cui ne è venuto a conoscenza, inviando una comunicazione a uno dei seguenti indirizzi (privacy@asst-rhodense.it; responsabileprotezionedati@asst-rhodense.it), cooperando, peraltro, al riguardo con il Titolare del trattamento al fine di adottare in modo immediato o, comunque, senza alcun indebito (ed ingiustificato) ritardo tutte le misure necessarie al fine di minimizzare i rischi derivanti dalla violazione per i soggetti interessati, porre rimedio al data breach e mitigarne qualsiasi ulteriore effetto negativo;
i. Assistere il Titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati (DPIA) ex art. 35 del GDPR e, in via eventuale, cooperare con il Titolare del trattamento nell'ambito dell'esecuzione degli oneri previsti dall'art. 36 del GDPR;
j. Al termine del contratto descritto al precedente punto 1.2.), il Responsabile del trattamento è tenuto a restituire tutti i dati personali al Titolare del trattamento e cancellare le copie esistenti, a meno che il diritto dell'UE o dei relativi Stati membri imponga la conservazione dei dati personali in questione, da ottemperare tuttavia nel rispetto del principio di minimizzazione ex art. 5 paragrafo 1) lettera c) del GDPR[4];
k. Mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al GDPR ed alla connessa normativa nazionale applicabile in materia, e consentire a

[2] L'elenco delle persone a cui è stato concesso l'accesso ai dati personali deve essere, altresì, sottoposto ad una revisione periodica, onde così verificare l'opportunità di revocare eventuali privilegi di accesso, invero, non più necessari. Inoltre, il Responsabile del trattamento è tenuto, su richiesta del Titolare, a dimostrare che le persone autorizzate al trattamento siano realmente soggette ai descritti obblighi di riservatezza.
[3] In tal caso, il Titolare del trattamento precisa che il Responsabile del trattamento deve scegliere un (sub) Responsabile del trattamento che rispetti i parametri di assessment di cui alla nota n. 3) del contratto, gli oneri di cui all'art. 2 del contratto nonché, infine, le istruzioni di cui al relativo allegato 3).
[4] Nel caso in cui una specifica disposizione normativa nazionale o comunitaria imponga al Responsabile del trattamento la conservazione dei dati personali trattati in nome e per conto del Titolare del trattamento, il primo si impegna a svolgere tale operazione di trattamento esclusivamente per la finalità e per la durata prevista dal relativo atto normativo.

quest'ultimo di svolgere, ove ritenuto opportuno o necessario, un'attività di revisione nei confronti del Responsabile del trattamento, ivi incluse le ispezioni, da realizzarsi ad opera del Titolare del trattamento ovvero da parte di un altro soggetto da questi appositamente incaricato;

l. Informare, in modo immediato o comunque senza indebito ritardo, il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR ovvero altre disposizioni normative, anche nazionali, applicabili in materia;
m. Curare, ove richiesto, assieme al Titolare del trattamento l'eventuale rapporto con la competente Autorità di Controllo ovvero l'organo giurisdizionale, anche in caso di eventuali procedimenti amministrativi, civili e/o penali;
n. Rispettare le disposizioni di cui al capo V) del GDPR (e connesse pronunce giurisprudenziali, dottrina ed atti di soft law), in caso di trasferimento di dati personali al di fuori del SEE o verso organizzazioni internazionali, previo ottenimento dello specifico nulla osta e relative istruzioni ad opera del Titolare del trattamento; nel caso in cui il trasferimento al di fuori del SEE o verso organizzazioni internazionali sia richiesto (o comunque imposto) da una legislazione comunitaria o di uno Stato membro dell'UE, il Responsabile del trattamento è tenuto ad informare, prima di svolgere tale operazione di trattamento, il Titolare del trattamento di tale requisito legale, a meno che la disposizione normativa in questione non vieti tale tipologia di comunicazioni ai fini di interesse pubblico.

3. Durata e corrispettivo.

3.1. Il presente Contratto è da considerarsi valido ed efficace a decorrere dalla data di validità e di efficacia del contratto descritto al precedente punto 1.2.); esso, tuttavia, perderà di efficacia e di validità in caso di cessazione, per qualsivoglia motivo, del contratto descritto al precedente punto 1.2.).

3.2. L'attività di trattamento, resa dal Responsabile del trattamento in favore del Titolare del trattamento, disciplinata dal presente Contratto di nomina, da ulteriori eventuali istruzioni, per iscritto, da parte del Titolare del trattamento nonché dalle ulteriori disposizioni normative nazionali/comunitarie applicabili è da intendersi a titolo gratuito, in deroga all'art. 1709 c.c.

4. Esonero di responsabilità.

4.1. Il Responsabile del trattamento si impegna, infine, a tenere indenne il Titolare del trattamento da qualsivoglia pregiudizio o responsabilità, anche in via indiretta ovvero parziale, derivante dalla violazione, ad opera del primo, degli oneri illustrati al precedente art. 2, delle ulteriori istruzioni eventualmente comunicate ovvero di qualsivoglia normativa applicabile alle operazioni di trattamento indicate nel Contratto ovvero connesse, anche in via indiretta, al contratto di cui al precedente punto 1.2.).

5. Disposizioni finali.

5.1. L'eventuale invalidità, inapplicabilità o inefficacia di alcune delle clausole che compongono il presente Contratto non determina, di conseguenza, l'invalidità, inapplicabilità o l'inefficacia integrale del Contratto medesimo.

5.2. Le Parti concordano che eventuali controversie circa l'interpretazione della validità, applicabilità od efficacia del presente Contratto sono devolute, in via esclusiva, alla competenza giurisdizionale del Foro di Milano.

Garbagnate Milanese (MI), lì ……

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE
(in persona del suo legale rappresentante pro tempore)

……

(in persona del suo legale rappresentante pro tempore)

……

Allegato 1) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679: informazioni sulle attività di trattamento.

1.1. Natura/finalità dell'attività di trattamento.
Le operazioni di trattamento che il Responsabile del trattamento può eseguire sulle tipologie di dati personali sono connesse, anche in via indiretta, a dare esecuzione al contratto tra le Parti descritto al punto 1.2.) del Contratto di nomina in questione.

1.2. Categoria dei soggetti interessati e relativa tipologia di dati personali.
Le informazioni personali (e relativi soggetti interessati) volte a dare compiuta esecuzione al contratto tra le Parti descritto al punto 1.2.) del Contratto di nomina in questione.

Allegato 2) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679: (sub) Responsabili del trattamento autorizzati.

Ai sensi dell'art. 2.1. lettera b) del Contratto di nomina, il Titolare del trattamento autorizza il Responsabile del trattamento ad utilizzare i seguenti (sub) Responsabili del trattamento:

Denominazione	Sede	Attività di trattamento delegata

A tal riguardo, si ricorda che il Titolare del trattamento autorizza, sin dalla data di efficacia e validità del presente Contratto, il Responsabile del trattamento ad utilizzare i sopra descritti (sub) Responsabili del trattamento, i quali non possono, tuttavia, effettuare (direttamente ovvero per il tramite di un altro (sub) Responsabile del trattamento) un'attività di trattamento differente da quella sopra concordata ed autorizzata, in assenza di una specifica ed esplicita autorizzazione da parte del Titolare.

Allegato 3) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679: misure di sicurezza tecniche ed organizzative.

Il Titolare consiglia al Responsabile del trattamento di implementare le seguenti misure di sicurezza[5], in conformità con i più importanti standard (dottrina, giurisprudenza ed atti di soft law) del settore (nel caso, il Responsabile del trattamento è tenuto a far sì che le descritte misure di sicurezza vengano rispettare anche dagli eventuali (sub) Responsabili del trattamento indicati nell'allegato 2) ovvero successivamente nominati in base all'art. 2.1. lettera d) di sopra):

a. Tutto il personale – ivi inclusi, ove opportuno, i collaboratori – deve ricevere un'adeguata sensibilizzazione, istruzione, formazione, addestramento e aggiornamento periodico sulle politiche di sicurezza delle informazioni anche personali implementate, sulle procedure (e prassi) organizzative nonché sulla normativa comunitaria e nazionale sulla protezione dei dati personali ("addestramento, awareness e formazione del cd. fattore umano")[6]. Inoltre, ove ritenuto opportuno dovrebbe essere istituito un processo disciplinare, formale e comunicato, volto ad intraprendere provvedimenti nei confronti del personale che ha commesso, con dolo o colpa grave, una violazione della sicurezza delle informazioni anche personali (data breach e/o incidente di sicurezza), della normativa comunitaria e nazionale sulla protezione dei dati personali ovvero di qualsivoglia altra normativa applicabile.
b. È stata predisposta una politica che mira a disciplinare, in modo compiuto, l'ipotesi di cessazione ovvero di variazione di responsabilità, durante il rapporto di lavoro o di collaborazione, di un soggetto autorizzato al trattamento[7].
c. I dati personali, oggetto di trattamento, devono essere archiviati mediante l'utilizzo di misure idonee a proteggerli da accessi non autorizzati, alterazioni, danni o distruzioni. Inoltre, il Responsabile del trattamento è tenuto a far sì che tutto il personale (e i collaboratori, ove opportuno) è tenuto a restituire gli asset utilizzati ed in loro possesso, al termine del periodo di impiego o del contratto stipulato, fatti salvi differenti e specifici accordi.
d. Viene implementato un sistema di autorizzazione dei profili di accesso[8], in base a ruoli e responsabilità (RBAC: Role Based Access Control): i) i profili di autorizzazione devono essere definiti e configurati dall'inizio del trattamento in modo da consentire l'accesso ai dati strettamente necessari (principio del "need to know"/"least privilege")[9]; ii) i profili di autorizzazione devono essere revisionati con cadenza periodica grazie ad un'apposita politica di accessi e di autorizzazione, da aggiornare sulla base dei requisiti di business ovvero di sicurezza delle informazioni (es. processo formale di registrazione e di de-registrazione per abilitare l'assegnazione dei diritti di accesso; processo formale per l'assegnazione o la revoca dei diritti di accesso per le utenze e i sistemi e/o servizi; limitazione e controllo dell'assegnazione e uso dei diritti di accesso privilegiato; rimozione dei diritti di accesso al momento della cessazione del rapporto di lavoro/di

[5] Tali misure possono, tuttavia, essere soggette ad una revisione (o meglio, una integrazione), tenuto conto della natura, della portata, del contesto e delle finalità delle attività di trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche interessate.
[6] È necessario sensibilizzare e rendere consapevoli dei rischi tutti gli operatori che possono accedere ai dati o ad altre risorse attraverso l'uso dei vari dispositivi; in modo particolare, alcuni utenti come gli amministratori di sistema oppure i dirigenti, cioè utenti con privilegi più elevati, devono comprendere l'importanza, i rischi e le responsabilità che derivano dal loro ruolo. È di fondamentale importanza sviluppare una corretta cultura della sicurezza in tutto il personale, indipendentemente dalle sue responsabilità, per poi considerare, con particolare attenzione, i ruoli critici; tutti devono avere una consapevolezza dei rischi e della propria capacità di prevenire incidenti di sicurezza (e/o data breach) e/o di gestirli e delle insidie che sia la quotidianità sia gli eventi fuori dall'ordinario possono generare. La formazione deve essere appropriatamente progettata in base ai ruoli e alle competenze pregresse del personale, su argomenti diversificati e identificati al bisogno.
[7] Le responsabilità e i doveri di sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio di impiego devono essere definiti, comunicati al relativo personale dipendente o al contraente, e fatti rispettare. I cambiamenti di responsabilità o di impiego dovrebbero essere gestiti come la cessazione delle responsabilità o dell'impiego attuale combinata con l'inizio di una nuova responsabilità o dell'impiego.
[8] I controlli d'accesso sono sia logici che fisici, e questi dovrebbero essere considerati insieme. Tale politica dovrebbe tener conto, inter alia, dei seguenti elementi: requisiti di sicurezza delle applicazioni aziendali; politiche per la diffusione e l'autorizzazione delle informazioni, per esempio il principio della necessità di sapere e i livelli di sicurezza delle informazioni e la loro classificazione; segregazione dei ruoli di controllo dell'accesso; requisiti per l'autorizzazione formale delle richieste di accesso, per la revisione periodica e la rimozione dei diritti di accesso; ruoli con accesso privilegiato.
[9] Le credenziali di accesso devono essere individuali per gli "user" e devono rispettare il principio di segregazione delle funzioni.

collaborazione ovvero adozione, modifica, integrazione o revisione ad ogni variazione[10]); iii) i compiti e le aree di responsabilità in conflitto tra loro devono essere oggetto di separazione, al fine di ridurre la possibilità di uso improprio, modifica non autorizzata o non intenzionale dei dati personali[11].

e. L'accesso ai sistemi e alle applicazioni viene controllato da procedure di log-in sicure.
f. I sistemi di gestione delle password devono essere interattivi, devono assicurare che le stesse siano di qualità (dunque siano adeguatamente complesse), e che siano opportunamente conservate e protette da accessi o utilizzi ad opera di soggetti non autorizzati.

   A tal fine, il Responsabile del trattamento deve assicurare la sussistenza dei seguenti requisiti:

   - ✓ richiesta, in via automatica, di aggiornamento periodico della password (non oltre 90 giorni) nei confronti di tutti i soggetti autorizzati al trattamento;
   - ✓ segretezza della password, la quale deve possedere, a tal fine, le seguenti caratteristiche minime:
     i. deve contenere almeno 12 caratteri[12] o, al più, 8 caratteri[13] ovvero, nel caso in cui lo strumento elettronico non lo permetta, un numero di caratteri pari al massimo consentito[14];
     ii. deve contenere lettere minuscole e maiuscole, combinate con cifre o caratteri speciali;
     iii. non deve contenere l'ID dell'utente, o comunque elemento agevolmente riconducibile a quest'ultimo;
     iv. deve essere modificata autonomamente ed obbligatoriamente dal soggetto autorizzato al primo collegamento, dopo l'eventuale re-impostazione, nel rispetto della cadenza temporale sopra descritta, nonché nel rispetto del criterio "password history" (ossia, impossibilità di riutilizzare, a breve distanza di tempo, le credenziali già precedentemente utilizzate);
     v. ove possibile, deve essere costituita dalla cd. "passphrase" (ossia, una raccolta di parole comuni casuali combinate in una frase che fornisca un'ottima combinazione di memorizzazione e sicurezza) ovvero a multi-fattori o strong authentication (MFA) (es. token; dato biometrico; informazione personale e riservata; OTP)[15].
   - ✓ la password deve essere conservata in modo sicuro, evitando la proliferazione di documenti non protetti contenenti liste di credenziali o appunti facilmente accessibili da chiunque;
   - ✓ le credenziali di autenticazione, collegate alla relativa password, devono essere disattivate se non utilizzate, in modo totale, da almeno 6 mesi o 1 anno, a seconda delle specifiche circostanze (e ad eccezione di quelle esplicitamente autorizzate)[16];

---

[10] Le identità digitali e le credenziali di accesso agli "user", i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza.

[11] L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.

[12] Cfr. sul punto: a) documento "2016 Italian Cybersecurity Report. Controlli Essenziali di Cybersecurity" già citato: "Le recenti best practice suggeriscono di forzare gli utenti a scegliere password lunghe almeno 12 caratteri, che contengano almeno un numero e un carattere non alfanumerico e che non contengano termini noti del vocabolario o informazioni facilmente riconducibili all'utente (es. nomi di familiari, animali domestici, date di anniversari e qualunque informazione possa essere facilmente trovata sui social network). L'uso di password complesse protegge l'utente nel caso in cui un attaccante riuscisse a impossessarsi di un database di password codificate, dato che renderebbe molto costoso per l'attaccante cercare di identificare le password provando tutte le combinazioni possibili (il cosiddetto "attacco a forza bruta")"; b) CNIL, Delibera n. 12 del 19.1.20217.

[13] Cfr. sul punto, Provvedimento n. 49 del 11.2.2021 a firma del Garante Privacy italiano [doc. web n. 9532852]: "...capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo".

[14] Cfr. punto n. 5) dell'abrogato Allegato B) del previgente Codice Privacy: "La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito…".

[15] Cfr., in via analogica, art. 1 comma 1) lettera q-bis) del Decreto Legislativo n. 11 del 17.1.2010: "autenticazione forte del cliente": "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (cfr. sul punto anche: Considerando n. 6) del Regolamento UE n. 389/2018 del 27.11.2017).

[16] Cfr., sul punto, l'abrogato Allegato B) (denominato "Disciplinare tecnico in materia di misure minime di sicurezza") del previgente D.Lgs. n. 196/2003 (Codice Privacy).

- ✓ la password deve essere tutelata mediante impostazioni idonee a contrastare efficacemente attacchi informatici di tipo "brute force" sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione (rate limiting)[17].

g. Viene attuata la protezione delle credenziali di autenticazione con efficaci misure di sicurezza crittografiche[18].
h. Viene assicurata la sicurezza fisica agli uffici, locali ed impianti che racchiudono dati personali, ivi inclusa la protezione da incidenti ovvero attacchi malevoli ("controllo di accesso fisico")[19].
i. Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce (ivi incluso, il malfunzionamento alla rete elettrica di alimentazione) e/o da accesso non autorizzato (interno o esterno), e le stesse devono essere, altresì, correttamente manutenute.
j. I supporti fisici, al cui interno sono archiviati dati personali, devono essere protetti da idonee misure di sicurezza contro accessi non autorizzati, utilizzi impropri ovvero manomissioni[20]; inoltre, il personale dipendente e, ove opportuno, i collaboratori devono assicurare che le apparecchiature lasciate incustodite siano, comunque, adeguatamente protette.
k. Viene adottata una politica di "scrivania pulita" (clear desk) per i documenti e i supporti di memorizzazione rimovibili (es. pendrive USB), e una politica di "schermo pulito" (clear screen) per i servizi di elaborazione delle informazioni[21].
l. Vengono controllati i cambiamenti all'interno dell'organizzazione, dei processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che influenzano la sicurezza delle informazioni ("gestione del cambiamento")[22].
m. E' stata predisposta una politica volta alla protezione dei dati da qualsivoglia software dannoso (virus/malware/ransomware[23]), da accessi remoti da rete pubblica da parte di sistemi non autorizzati, nonché

[17] Il "rate limiting" è una misura di sicurezza tecnica che comporta una limitazione al numero di tentativi infruttuosi di autenticazione costituendo un'efficace protezione dagli attacchi di "denial of service" (DDOS), dai tentativi di violazione delle password con metodi "brute force" e da altri comportamenti illegali: di conseguenza, tale misura provvede a limitare o rallentare la disponibilità di una procedura di login, qualora si verifica una quantità anomala di tentativi di accesso non andati a buon fine in un intervallo di tempo relativamente ristretto, procedendo, quindi, a bloccare temporaneamente i login per l'account sotto attacco; tale misura potrebbe, altresì, prevedere un incremento delle tempistiche di blocco, qualora si riscontrassero nuovi tentativi di accesso falliti dopo lo sblocco dell'account, preferibilmente per non più di un paio d'ore, al fine di non impedire l'accesso al servizio.
[18] In merito, è opportuno che una politica sull'uso, la protezione e la durata delle chiavi crittografiche dovrebbe essere sviluppata e implementata attraverso il loro intero ciclo di vita.
[19] L'accesso fisico alle risorse deve essere protetto ed amministrato. Nello specifico, le relative linee guida dovrebbero prevedere, inter alia, le seguenti prescrizioni: i perimetri di sicurezza dovrebbero essere definiti, e l'ubicazione e la forza di ogni perimetro dovrebbe dipendere dai requisiti di sicurezza degli asset all'interno del perimetro e dai risultati di una valutazione dei rischi; i perimetri di un edificio o di un sito contenente strutture per l'elaborazione delle informazioni dovrebbero essere fisicamente solidi e custoditi; un'area di accoglienza presidiata o altri mezzi per controllare l'accesso fisico al sito o all'edificio dovrebbe essere in atto, e limitato solo al personale autorizzato; adeguati sistemi di rilevamento delle intrusioni dovrebbero essere installati.
[20] La documentazione deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedure di tracciamento delle chiavi in uso.
[21] La politica di clear desk/clear screen dovrebbe, inter alia, considerare i seguenti aspetti: le informazioni aziendali sensibili o critiche dovrebbero essere chiuse a chiave quando non sono necessarie, specialmente quando l'ufficio è lasciato libero; i computer e i terminali dovrebbero essere lasciati scollegati o protetti con un meccanismo di blocco dello schermo e della tastiera controllato da una password, un token o un meccanismo simile di autenticazione dell'utente quando non sono sorvegliati, e dovrebbero essere protetti da password o altri controlli quando non sono in uso. Una politica di clear desk/clear screen riduce i rischi di accesso non autorizzato, perdita e danno alle informazioni durante e al di fuori del normale orario di lavoro; invece, casseforti o altre forme di archiviazione sicura potrebbero anche proteggere le informazioni ivi conservate da disastri come un incendio, un terremoto, un'inondazione o un'esplosione.
[22] I cambiamenti nell'organizzazione, nei processi di business, nelle strutture di elaborazione delle informazioni e nei sistemi che influiscono sulla sicurezza delle informazioni devono essere controllati. In particolare, devono essere considerati i seguenti elementi: identificazione e registrazione dei cambiamenti significativi; valutazione degli impatti potenziali, compresi gli impatti sulla sicurezza delle informazioni anche personali, di tali cambiamenti; verifica che i requisiti di sicurezza delle informazioni siano stati soddisfatti; comunicazione dei dettagli del cambiamento a tutte le persone interessate; procedure di fall back.

è stato predisposto un sistema di protezione delle postazioni terminali (endpoint protection systems – EPS): i) i programmi di protezione anti virus e anti malware devono essere continuamente aggiornati; ii) gli aggiornamenti delle patch di sicurezza e le correzioni per le vulnerabilità di sistema note devono essere prontamente implementate; iii) i sistemi perimetrali, quali firewall[24], devono essere presenti, aggiornati, mantenuti, ben configurati e rivisti periodicamente.

n. E' stata predisposta una procedura di backup[25] (crittografato, ove possibile) volta a garantire il recupero dei dati e il ripristino dei sistemi in caso di incidenti di sicurezza, data breach, anomalie o altri eventi dannosi: i) la copia dei dati e delle configurazioni dei sistemi deve essere eseguita almeno su base giornaliera ove possibile; ii) la retention di tali copie deve essere pari ad almeno una settimana, salvo richieste differenti che potranno essere concordate nella fase contrattuale o nel corso dell'esecuzione del servizio di cui al punto 1.2.) del Contratto; iii) le copie dei dati devono essere protette da accessi non autorizzati e conservate in un luogo sicuro, preferibilmente offline; iv) deve essere garantita l'integrità delle copie dei dati e il funzionamento delle procedure di restore da testare con regolarità.
o. Le attività degli Amministratori di Sistema (AdS)[26] vengono sottoposte ad audit log[27], conservati, protetti e riesaminati in modo periodico, nel rispetto del Provvedimento del 27.11.2008 del Garante Privacy, così come modificato in base al successivo Provvedimento del 25.6.2009.
p. Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata, e appropriate misure devono essere intraprese per affrontare i rischi relativi (cd. gestione delle vulnerabilità tecniche).
q. Le reti devono essere gestite e controllate al fine di proteggere le informazioni nei sistemi informativi e nelle applicazioni software.
r. Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato (es. antispam; mail filter[28]).

---

[23] Si definisce "malware" qualsiasi software che, una volta eseguito su un sistema informatico, possa apportare modifiche indesiderate o danni al sistema stesso e ai suoi utenti; i malware possono effettuare le azioni più diverse sul sistema "vittima", quali ad esempio: possono sottrarre le informazioni memorizzate, danneggiarle o modificarle in maniera ponderata; catturare schermate del dispositivo "vittima" violando la privacy dei suoi utenti; rubare le credenziali degli utenti che usano il sistema. Invece, i "ransomware" rappresentano una tipologia specifica di malware il cui obiettivo è quello di impedire alla vittima l'accesso e l'uso di documenti e dispositivi.
La politica contro il malware dovrebbe essere basata sul software di rilevamento e riparazione del malware, sulla consapevolezza della sicurezza delle informazioni e su controlli appropriati dell'accesso al sistema e della gestione dei cambiamenti. La relativa guida dovrebbe almeno: stabilire una politica formale che proibisca l'uso di software non autorizzato; implementazione di controlli che impediscano o rilevino l'uso di un software non autorizzato; implementare controlli che impediscano o rilevino l'uso di siti web maligni noti o sospetti; condurre revisioni regolari del contenuto del software e dei dati dei sistemi che supportano i processi aziendali critici: la presenza di qualsiasi file non approvato o modifiche non autorizzate dovrebbe essere formalmente indagata.

[24] Il "firewall" è un componente che si interpone tra due reti, e permette di imporre regole sul transito di informazioni tra queste.

[25] Quando si progetta un piano di back up, almeno i seguenti elementi dovrebbero essere presi in considerazione: devono essere prodotte registrazioni accurate e complete delle copie di back up e delle procedure di ripristino documentate; i back up dovrebbero essere conservati in un luogo remoto, ad una distanza sufficiente per sfuggire a qualsiasi danno di un disastro nel sito principale; le informazioni di back up dovrebbero ricevere un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati al sito principale; i supporti di back up dovrebbero essere testati regolarmente, al fine di garantire che si possa fare affidamento su di essi quando necessario; nelle situazioni in cui la riservatezza è importante, i back up dovrebbero essere protetti con mezzi di crittografia.

[26] Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate a: gestione e manutenzione di un impianto di elaborazione o di sue compenti (es. salvataggio dei dati; organizzazione dei flussi di rete; gestione dei supporti di memorizzazione; manutenzione degli hardware) (cd. AdS di una infrastruttura informatica); gestione e manutenzione di un sistema operativo; gestione e manutenzione di uno o più applicativi (es. data base; antivirus) (cd. AdS degli applicativi). Inoltre, si ricorda che, nel rispetto del citato Provvedimento del Garante Privacy italiano, gli estremi identificativi delle persone fisiche qualificate come "amministratori di sistema" devono essere riportati in un documento interno da mantenere aggiornato.

[27] Audit log: consiste nel log sulle attività svolte all'interno di uno specifico sistema/apparato informativo; esso si differenzia dall'"access log", il quale riguarda, invece, i log di entrata e di uscita da un determinato sistema informativo.

[28] È un componente che intercetta ogni mail in transito verso l'azienda, al fine di identificare e bloccare tempestivamente possibili minacce.

s. È stata stabilita la responsabilità e la procedura di gestione volta ad assicurare una risposta rapida, efficace ed ordinata agli incidenti di sicurezza e/o agli incidenti relativi alla sicurezza delle informazioni personali: tali eventi devono essere segnalati il più velocemente possibile, tramite appropriati canali gestionali. A tal fine, il personale dipendente e, ove opportuno, i collaboratori che utilizzano i sistemi informativi e i servizi dell'organizzazione devono essere tenuti a registrare e a segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.
t. I piani di ripristino (recovery plan)[29], la conoscenza acquisita dall'analisi e dalla soluzione degli incidenti costituenti la violazione di dati personali (data breach) o della sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto di incidenti futuri ("lesson learned").
u. E' stata predisposta una procedura di risposta (Incident Response e Business Continuity, nel rispetto della ISO/IEC 22301:2014) e di recupero (Incident Recovery e Disaster Recovery[30]), al fine di fronteggiare un incidente, un evento imprevisto o di forza maggiore ovvero un disastro[31]; le descritte procedure devono essere, altresì, verificate ad intervalli di tempo regolari, al fine così di assicurare che siano sempre valide ed efficaci durante il verificarsi di una situazione avversa, di crisi o comunque imprevista.
v. I dati personali, oggetto dell'attività di trattamento demandata dal Titolare al Responsabile, vengono distrutti, cancellati, sovrascritti o comunque resi inutilizzabili (o in alcun modo ricostruibili) in modo irreversibile, in caso di sostituzione di un hardware/software o in caso di riutilizzo, per differenti finalità di trattamento, dell'hardware/software medesimo.
w. È stato predisposto un sistema di prevenzione delle intrusioni (intrusion prevention systems[32] – IPS), da tenere aggiornato, mantenuto, ben configurato e rivisto periodicamente.
x. Viene svolto, con cadenza periodica, il monitoraggio della rete informatica al fine di rilevare potenziali eventi di cybersecurity[33].
y. Viene attuata la protezione delle comunicazioni di dati in transito (data in transit) con tecniche crittografiche allo stato dell'arte.
z. Vengono effettuate delle sessioni di vulnerability assessment e penetration test (VAPT) sui sistemi/applicativi coinvolti nell'esecuzione delle attività di trattamento di cui al Contratto, da eseguirsi con cadenza regolare e periodica, anche ad opera, ove necessario, di terze parti indipendenti.

[29] I processi e le procedure di ripristino devono essere eseguiti e mantenuti al fine di assicurare un recupero dei sistemi o asset coinvolti da un incidente di sicurezza e/o da una violazione dei dati personali (data breach).
[30] Cfr., in via analogica, il Provvedimento n. 333 del 4.7.2013 a firma del Garante Privacy italiano: "…con il termine "disaster" si intende, ai fini del provvedimento in esame, "l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione", laddove la nozione di DR configura invece "l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro di elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare indisponibilità prolungate". Il DR comprende quindi le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e di servizi di comunicazione".
[31] A tal fine, deve sussistere un documento aggiornato di dettaglio contenente i piani di continuità operativa/disaster recovery, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: le politiche e i processi impiegati per identificare le priorità degli eventi; le fasi di attuazione dei piani; i ruoli e le responsabilità del personale; i flussi di comunicazione e reportistica.
[32] È un componente che controlla in modo continuo il traffico e le attività in essere nella rete aziendale per identificare e, laddove possibile, prevenire possibili intrusioni non autorizzate.
[33] Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity.