

ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI - DATA PROCESSING AGREEMENT

(ai sensi dell'art. 28 del Regolamento UE 2016/679)

CLAUSOLE CONTRATTUALI STANDARD

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

- a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- b) Il titolare del trattamento e il responsabile del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.
- c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
- d) Gli allegati da I a IV costituiscono parte integrante delle clausole.
- e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.
- f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

Clausola 2

Invariabilità delle clausole

- a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.
- b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

- a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.
- b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679, rispettivamente.

c)Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5

Clausola di adesione successiva

- a)Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.
- b)Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.
- c)L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II

OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7

Obblighi delle parti

7.1. Istruzioni

- a)Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale 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. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, 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.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

- d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.
- e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

- a) Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 30 giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.
- b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.
- c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
- d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.
- e) 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.

7.8. Trasferimenti internazionali

- a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata 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.
- b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 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.

Clausola 8

Assistenza al titolare del trattamento

- a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.
- b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.
- c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:
 - 1) 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;
 - 2) 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;
 - 3) l'obbligo di 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;
 - 4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.
- d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. 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'adempire, in conformità dell'articolo 34 del regolamento (UE) 2016/679, 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.

9.2. 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 senza ingiustificato ritardo dopo esserne venuto a conoscenza. 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 III 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 (UE) 2016/679.

SEZIONE III

DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle clausole e risoluzione

- a) Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
- b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:
- 1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
 - 2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
 - 3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.
- c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.
- d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I

Elenco delle parti

Titolare del trattamento

Il soggetto che, ai sensi del presente Accordo sul trattamento dei dati personali (DPA), risulta designato come titolare.

Responsabile del trattamento

Nome: SSI-COM Srl

Indirizzo: Via Giotto, 7, 20145 Milano MI

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati:

- Soggetti terzi i cui Dati personali sono di titolarità del Titolare del trattamento
- Clienti del Titolare del Trattamento
- Fornitori del Titolare del Trattamento coinvolti nell'esecuzione del contratto
- Dipendenti/ Collaboratori del Titolare del Trattamento
- Utenti delle pagine social del Titolare del Trattamento
- Altre eventuali categorie di Soggetti interessati

Categorie di dati personali trattati:

- Dati personali comuni (a titolo esemplificativo dati anagrafici e di contatto)
- Dati contrattuali, retributivi, contributivi e fiscali
- Tutte le categorie di Dati messe a disposizione del Responsabile da parte del Titolare del trattamento e il cui trattamento è necessario per l'erogazione dei Servizi
- Altre eventuali categorie di Dati personali

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari:

Dati sensibili trattati:

- Categorie particolari di dati ai sensi degli artt. 9 e 10 del GDPR

- Il trattamento delle categorie particolari di dati personali è effettuato esclusivamente da personale debitamente autorizzato e specificamente formato in materia di protezione dei dati personali e sicurezza informatica

Natura del trattamento:

La natura del trattamento consiste nella gestione, da parte del Responsabile del trattamento, dei dati personali dei Soggetti terzi i cui Dati sono di titolarità del Titolare per erogare i Servizi previsti dal Contratto stipulato tra le parti.

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento:

Il Responsabile del Trattamento tratta i Dati Personali dei Soggetti interessati esclusivamente per erogare i Servizi previsti dal Contratto stipulato tra le parti.

Durata del trattamento:

I Dati saranno conservati per tutta la durata del Contratto stipulato tra le parti. Dopo la risoluzione del Contratto, il Responsabile del trattamento, a scelta del Titolare del trattamento, procederà alla cancellazione di tutti i Dati personali trattati per conto del Titolare oppure alla restituzione di tutti i Dati personali al Titolare e alla cancellazione delle copie esistenti, salvo che il diritto dell'Unione o dello Stato membro richieda la conservazione dei Dati personali. Finché i Dati non sono cancellati o restituiti, il Responsabile del trattamento continuerà ad assicurare il rispetto delle presenti clausole.

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento:

I sub-responsabili nominati dal Responsabile del trattamento:

- effettuano le medesime operazioni di trattamento descritte sopra, necessarie per l'erogazione dei Servizi previsti dal Contratto;
- trattano le stesse categorie di dati personali sopra indicate;

conservano i dati personali per la medesima durata prevista per il Responsabile del trattamento nelle presenti Clausole e sono tenuti alle stesse procedure di cancellazione o restituzione al termine del trattamento.

ALLEGATO III**Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati****Misure di pseudonimizzazione e cifratura dei dati personali**

1. Cifratura degli hard disk dei dispositivi aziendali tramite Bitlocker
2. Crittografia dei log operativi sul software di gestione e analisi dei log AdS e operativi
3. Crittografia delle password (utilizzo del software Keeper per la gestione delle password)

Misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

1. Accesso degli utenti tramite username e password nominativi
2. Attivazione e utilizzo della 2FA ove disponibile
3. Controllo degli accessi robusto gestito tramite Microsoft AD
4. Policy del “minimo privilegio” per l’accesso ai dati, “clean desk policy” e “policy BYOD”.
È stata inoltre adottata una specifica policy per prevenire eventuali violazione dei dati in caso di remote working dell’incaricato.
5. Segregazione delle reti in differenti VLAN
6. Sistemi operativi, software e applicativi sono periodicamente aggiornati ed è stata adottata una policy di “patch management”

Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

1. Gestione e analisi dei log operativi
2. Analisi semestrale dell’operato degli amministratori di sistema (AdS)
3. Sono conservati gli access log degli amministratori di sistema in ottemperanza al provvedimento del Garante per la Protezione dei Dati Personali e viene effettuata periodica attività di audit sugli stessi.
4. Analisi semestrale dei log degli amministratori di sistema
5. Sistemi operativi, software e applicativi sono periodicamente aggiornati ed è stata adottata una policy di “patch management”

Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

1. Presenza di UPS e gruppo elettrogeno diesel da utilizzare in caso di blackout superiore a 1 minuto.
2. È stata adottata una solida policy di backup al fine di prevenire eventuali incidenti che potrebbero portare all’indisponibilità e alla perdita dell’integrità dei dati
3. Sono state adottate linee idonee misure per garantire il ripristino dell’accesso ai dati in caso di incidente, in tempi certi, compatibili con i diritti degli interessati e comunque non superiori alle 48 ore.

Misure di identificazione e autorizzazione dell'utente

1. Accesso degli utenti tramite username e password nominativi
2. Attivazione e utilizzo della 2FA ove disponibile
3. Controllo degli accessi robusto gestito tramite Microsoft AD
4. Principio del minimo privilegio degli utenti

Misure di protezione dei dati durante la trasmissione

1. I dati vengono trasmessi esclusivamente su connessioni sicure https

Misure di protezione dei dati durante la conservazione

1. Presenza di un Firewall e utilizzo di un antivirus professionale che offre protezione avanzata all’azienda.
2. Gestione e analisi dei log operativi
3. Cifratura degli hard disk dei dispositivi aziendali tramite Bitlocker

Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

1. Accesso ai locali controllato
2. Presenza del registro degli accessi all'ingresso
3. La sala server è chiusa a chiave. La chiave è in possesso esclusivo dei responsabili IT che devono firmare apposito registro al momento dell'accesso al locale
4. Sono state adottate rigide procedure per la prevenzione degli incendi, dei blackout, degli sbalzi di tensione e degli accessi non autorizzati al perimetro aziendale.
5. È stata adottata un'apposita Policy di conservazione, stoccaggio e smaltimento documenti

Misure per garantire la registrazione degli eventi

1. Gestione e analisi dei log operativi
2. Analisi semestrale dell'operato degli amministratori di sistema (AdS)
3. Sono conservati gli access log degli amministratori di sistema in ottemperanza al provvedimento del Garante per la Protezione dei Dati Personali e viene effettuata periodica attività di audit sugli stessi.
4. Analisi semestrale dei log degli amministratori di sistema

Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita

1. Sistemi operativi, software e applicativi sono periodicamente aggiornati ed è stata adottata una policy di "patch management"
2. Cifratura degli hard disk dei dispositivi aziendali tramite Bitlocker

Misure di informatica interna e di gestione e governance della sicurezza informatica

1. Insieme di policy relative alla gestione sicura dei dati e dei processi che concernono il trattamento dei dati personali

Misure per garantire la minimizzazione dei dati

1. È stata adottata una policy relativa alla privacy by design che ha una determinata sezione relativa alla minimizzazione dei dati.

Misure per garantire la qualità dei dati

1. Presenza di un Firewall e utilizzo di un antivirus professionale che offre protezione avanzata all'azienda.
2. Gestione e analisi dei log operativi

Misure per garantire la conservazione limitata dei dati

1. È stata adottata una policy relativa alla data retention che prevede uno scadenziario preciso per tutte le categorie dei dati personali trattati

Misure per garantire la responsabilità

1. La società ha nominato, con apposito atto, tutti i soggetti autorizzati al trattamento dei dati personali, vincolandoli a un obbligo di riservatezza.

2. La società ha nominato, con apposita nomina o DPA, tutti i responsabili e i sub-responsabili del trattamento (art. 28 del GDPR)
3. La società ha nominato, con apposito atto, tutti gli amministratori di sistema (AdS)
4. Il personale riceve periodica formazione in materia di privacy e data protection e di cybersecurity.
5. Sono state adottate policy del “minimo privilegio” per l’accesso ai dati, “clean desk policy” e “policy BYOD”. È stata inoltre adottata una specifica policy per prevenire eventuali violazione dei dati in caso di remote working dell’incaricato.

Misure per consentire la portabilità dei dati e garantire la cancellazione

1. È stata adottata una policy relativa alla gestione dei diritti da parte degli interessati (compresa la portabilità dei dati);
2. È stata adottata un’apposita Policy di conservazione, stoccaggio e smaltimento documenti.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento

1. È stata adottata una policy relativa alla gestione dei diritti da parte degli interessati che disciplina anche l’eventualità di un supporto del Responsabile nei confronti del Titolare per la gestione di eventuali richieste;
2. È stata adottata una policy relativa alla gestione dei data breach che contiene le procedure che il Responsabile deve adottare nel caso in cui avvenga un data breach che coinvolge i dati del Titolare.

ALLEGATO IV

Elenco dei sub-responsabili del trattamento

La lista dei sub-responsabili del trattamento è fornita su richiesta.