Accordo

DPA per il trattamento dei dati personali

Sistemistica, Programmazione, Sviluppo e Gestionale

Addendum al Contratto concluso tra le parti

Versione: 01_2023

Premesse

Dal 1999 Joker S.r.L., grazie alle competenze specialistiche maturate, fornisce soluzioni informatiche e servizi di consulenza aziendale in ambito IT e Industria 4.0.

Si tratta di soluzioni per aziende, soluzioni IT e, in particolare, assistenza e consulenza informatica, noleggio hardware e software, sviluppo di applicativi e servizi, sicurezza informativa, sistemistica, programmazione e gestione di sistemi informativi. Partner di Zucchetti e Microsoft, lavora aggiornandosi costantemente, alla ricerca di soluzioni, sistemi e strumenti sempre più performanti per permettere alla propria clientela di migliorare processi e prestazioni.

Joker S.r.L., stante la natura delle proprie attività, considera la qualità e la sicurezza delle informazioni, inclusi i dati personali, un fattore irrinunciabile per la protezione del proprio patrimonio informativo ma anche e soprattutto di quello affidatole dai clienti.

L'azienda ha sviluppato un piano strategico che include l'identificazione dei rischi sulla sicurezza delle informazioni e l'implementazione di adeguate misure per mitigarli.

Il trattamento dei dati personali che i clienti affidano a Joker S.r.L. è un trattamento che, per lo più, ricade sotto le previsioni del c.d. Gdpr, 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).

Definizioni

Dato personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

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.

Archivio
Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Titolare del trattamento
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Destinatario
La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Terzo
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Consenso dell'interessato
Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Violazione dei dati personali
La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dati genetici
I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici
I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute
I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Decisione di adeguatezza
Indica una decisione della Commissione Europea resa ai sensi dell'art. 45, 3. del Gdpr in merito al fatto che la normativa di un dato Paese garantisce un livello adeguato di protezione dei dati personali.

Data di decorrenza dell'accordo o del contratto
La data in cui il Cliente sottoscrive o accetta la proposta o questo accordo o, se anteriore, la data di decorrenza del contratto che lo lega a Joker S.r.L.

Istruzioni
Si tratta delle istruzioni scritte che il Titolare impartisce al Responsabile (o il Responsabile impartisce al Sub Responsabile), incluse in questo Accordo.

Responsabile Ulteriore del trattamento o Sub Responsabile
Indica qualunque subappaltatore cui un Responsabile abbia subappaltato uno qualsiasi degli obblighi o dei trattamenti assunti contrattualmente e che, nell'esecuzione delle prestazioni subappaltate, potrebbe raccogliere, accedere, ricevere, conservare o comunque elaborare dati personali.

Servizio, Servizi o Prestazione
Indica quanto oggetto del contratto tra le parti.

Utente finale
Indica l'eventuale fruitore finale del servizio, di regola il cliente o l'interessato il cui trattamento dei dati è in capo al Titolare del trattamento.

*

Il Gdpr stabilisce che il trattamento di dati personali affidato da un soggetto, definito Titolare, ad un altro, definito Responsabile, deve essere disciplinato da un contratto o da altro atto giuridico.

Quando tratta dati personali per conto di un cliente Titolare, Joker S.r.L. assume la veste e la qualifica di Responsabile del trattamento ai sensi dell'art. 28 del Gdpr.

Si intenda, in caso, che se il Titolare rivestisse, invece, la qualifica o la veste di Responsabile, Joker, ai fini di questo documento, sarà allora da intendersi quale Sub-Responsabile, fermo restando che il potere di sub delegare i trattamenti indicati negli Allegati è di competenza e piena responsabilità di chi tali trattamenti delega.

Questo documento (DPA) precisa i diritti e gli obblighi delle parti in relazione ai Servizi richiesti a Joker S.r.L., che includono la raccolta, l'organizzazione, la strutturazione, l'archiviazione, l'utilizzo o la divulgazione di dati personali richieste nell'ambito della fornitura dei servizi prestati da Joker S.r.L. al Cliente.

I servizi e le prestazioni erogate da Joker riguardano le applicazioni, i prodotti e servizi e la consulenza che Joker offre, presta, progetta, sviluppa, utilizza e gestisce anche per conto del Cliente.

Articolo 1. Scopo e ambito di applicazione

a. Scopo di queste pattuizioni è garantire il rispetto dei requisiti della normativa in materia di protezione dei dati personali.
b. Il titolare e il responsabile del trattamento di cui all'Allegato 1 hanno accettato queste pattuizioni, che si applicano al trattamento dei dati personali specificato nell'Allegato 2.
c. L'appendice con gli Allegati è parte integrante di questo Accordo.

Articolo 2. Invariabilità delle pattuizioni

d. Le Parti si impegnano a non modificare il contenuto e la portata di questo Accordo e dei suoi Allegati tranne che per aggiungere o aggiornare informazioni nell'appendice.
e. Ciò non impedisce alle parti di includere le pattuizioni contrattuali tipo stabilite nelle presenti pattuizioni in un contratto più ampio e di aggiungere altre pattuizioni o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti o ledano i diritti o le libertà fondamentali degli interessati.
f. Queste pattuizioni non pregiudicano gli obblighi cui sono soggette le Parti a norma del regolamento (UE) 2016/679.

Articolo 3. Interpretazione

a) Quando queste pattuizioni utilizzano termini che sono definiti nel Regolamento (UE) 2016/679, i termini hanno il significato in esso stabilito.
b) Questi accordi vanno letti e interpretati alla luce delle disposizioni del Regolamento (UE) 2016/679.

Articolo 4. Gerarchia

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

Articolo 5. Descrizione dei trattamenti

I dettagli dei trasferimenti, in particolare le categorie di dati personali trasferiti e le finalità per le quali i dati sono trasferiti, sono specificati nell'Allegato 2.

Articolo 6

6.1. Istruzioni

a) Il Responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile informa il titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.
b) Il responsabile informa immediatamente il titolare qualora, a suo parere, le istruzioni di quest'ultimo violino il Regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

6.2. Limitazione delle finalità

Il responsabile tratta i dati personali soltanto per le finalità specifiche del trasferimento di cui all'allegato 2, salvo ulteriori istruzioni del titolare.

6.3. Durata del trattamento; cancellazione e restituzione dei dati

Il responsabile tratta i dati personali soltanto per la durata specificata nell'allegato 2. Al termine del trattamento il responsabile emette comunicazione formale in cui informa che da quel momento tutti i trattamenti dell'Accordo sono interrotti.

Al termine della prestazione dei servizi di trattamento il responsabile:

a) mantiene a disposizione del titolare i dati personali per l'estrazione o per la restituzione per 30 giorni successivi alla cessazione del rapporto;
b) provvede alla cancellazione dei dati personali (ivi incluse eventuali copie) dai sistemi del responsabile o da quelli su cui lo stesso abbia controllo entro il termine previsto nel Contratto, tranne il caso in cui la conservazione dei dati da parte del responsabile sia necessaria al fine di assolvere ad una disposizione di legge italiana o europea;
c) distrugge eventuali dati personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del responsabile sia necessaria ai fini del rispetto di norme di legge italiane o europee.

Fermo restando quanto altrimenti previsto in questo accordo, il titolare riconosce che è sua responsabilità provvedere all'estrazione totale o parziale dei dati personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui sopra. Parimenti il titolare riconosce che è propria responsabilità richiedere, se del caso, la consegna di copia di tali dati entro il medesimo termine di 30 giorni dalla cessazione del rapporto.

Quanto qui previsto non si applica ai rapporti aventi ad oggetto prodotti installati presso il titolare o presso fornitori del titolare.

Finché i dati non sono cancellati, distrutti o restituiti, il responsabile continua ad assicurare il rispetto di queste pattuizioni.

6.4. Sicurezza del trattamento

a) Il titolare prende atto e conviene che il responsabile del trattamento mette in atto le misure tecniche e organizzative specificate nell'allegato 3. Tali misure includono 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 hanno tenuto 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 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 garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
c) In caso di violazione dei dati personali trattati dal responsabile, questi adotta misure adeguate per porre rimedio alla violazione, anche per attenuarne gli effetti negativi. Informa il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Tale notifica contiene i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni, una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione), le sue probabili conseguenze e le misure adottate o di cui si propone l'adozione per

porre rimedio alla violazione, 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.

d) Il responsabile coopera con il titolare e lo assiste per consentirgli di adempiere agli obblighi che gli incombono a norma del Gdpr, in particolare di dare notifica all'autorità di controllo competente e agli interessati in questione, tenuto conto della natura del trattamento e delle informazioni di cui dispone l'importatore.

6.5. Categorie particolari di dati personali

Le Parti convengono che i Servizi prestati dal responsabile non sono destinati al trattamento di categorie particolari di dati personali (cc.dd. "sensibili"); se il titolare desiderasse affidare, anche solo in parte o sporadicamente, tali trattamenti al responsabile, dovrà ottenerne previa specifica autorizzazione, concordando con quest'ultimo tipologie, specificando finalità e i tempi di conservazione nonché le specifiche garanzie e misure tecniche da adottare.

In particolare, se il trattamento riguardasse 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 (cc.dd. dati sensibili), il responsabile del trattamento concorderà con il titolare l'applicazione di limitazioni specifiche e/o garanzie supplementari nell'allegato 3.

6.6. Documentazione e rispetto

Le parti devono essere in grado di dimostrare il rispetto di queste pattuizioni.

Il responsabile sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei dati personali trattati per conto del titolare e le sedi in cui avviene tale trattamento. Il responsabile ha facoltà di incaricare professionisti indipendenti per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report. Tali report, che costituiscono informazioni confidenziali del responsabile, potranno essere resi disponibili al titolare per consentirgli di verificare la conformità del responsabile agli obblighi di sicurezza di cui a questo Accordo.

Il diritto di verifica del titolare è esercitato attraverso la verifica dei report messi a disposizione dal responsabile. Quest'ultimo riconosce il diritto del titolare, con le modalità e nei limiti di seguito indicati, di effettuare audit indipendenti per verificare la conformità del responsabile stesso agli obblighi previsti in questo Accordo e/o dalla normativa. Il titolare potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.

In questi casi il titolare è tenuto a inviare richiesta scritta al responsabile. Successivamente alla richiesta di audit o ispezione il responsabile e il titolare concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il titolare e coloro che effettuano le verifiche e i costi che il responsabile potrà addebitare per tali verifiche, che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.

Il responsabile potrà opporsi per iscritto alla nomina da parte del titolare di eventuali revisori o consulenti esterni che siano, ad insindacabile giudizio del responsabile, non adeguatamente qualificati o indipendenti, siano concorrenti del responsabile o siano evidentemente inadeguati. In tali circostanze il titolare sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

Il titolare si impegna a corrispondere al responsabile gli eventuali costi documentati e comunicati nella fase sopra indicata, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del titolare i costi delle attività di verifica dallo stesso commissionate a terzi.

Queste pattuizioni non sono applicabili ai rapporti, contratti o patti aventi ad oggetto prodotti o servizi installati presso il titolare o presso fornitori del titolare.

Le attività di verifica presso sub responsabili indicati dal responsabile dovranno essere effettuate secondo le regole e le politiche da questi indicate.

6.7. Assistenza a fini di conformità

Il responsabile presterà assistenza al titolare e coopererà nei modi di seguito indicati al fine di consentire al titolare il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.

Qualora il responsabile riceva richieste o reclami da un Interessato in relazione ai dati personali trattati per conto del titolare, il responsabile raccomanderà all'Interessato di rivolgersi al titolare. In tali casi il responsabile informerà tempestivamente per iscritto il titolare del ricevimento della richiesta mediante e fornirà al titolare le informazioni ad esso disponibili unitamente a copia della richiesta stessa o del reclamo. Resta inteso che tale attività di cooperazione sarà svolta in via eccezionale, in quanto la gestione dei rapporti con gli Interessati resta esclusa dai servizi prestati dal responsabile ed è responsabilità generale del titolare gestire eventuali reclami in via diretta e garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il titolare stesso..

Qualora, ai fini dell'evasione delle richieste di cui ai precedenti punti, il titolare abbia necessità di ricevere informazioni dal responsabile circa il trattamento dei dati personali, il responsabile presterà la necessaria assistenza nei limiti di quanto ragionevolmente possibile, a condizione che tali richieste siano presentate con congruo preavviso.

Il responsabile provvederà a informare tempestivamente il titolare, salvo il caso in cui ciò sia vietato dalla legge, per iscritto, di eventuali ispezioni o richieste di informazioni presentate da autorità di controllo e forze di polizia rispetto a profili che riguardano il trattamento dei dati personali di cui a questo Accordo.

Il responsabile, tenuto conto della natura dei dati personali e delle informazioni ad esso disponibili, fornirà ragionevole assistenza al titolare nel rendere disponibili informazioni utili per consentire al titolare l'effettuazione di valutazioni di impatto sulla protezione dei dati personali nei casi previsti dalla legge. In tal caso il responsabile renderà disponibili informazioni di carattere generale in base al servizio effettivamente prestato, quali le informazioni contenute in questo Accordo e/o nei DPA eventualmente in essere. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del titolare. Resta inteso che è responsabilità e onere esclusivo del titolare procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei dati personali dallo stesso posto in essere. Quanto qui previsto non trova applicazione per i rapporti aventi ad oggetto prodotti installati presso il titolare o presso fornitori del titolare.

Il responsabile si impegna a rendere Servizi improntati ai principi di minimizzazione del trattamento (privacy by design & by default), fermo restando che è responsabilità esclusiva del titolare assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi e verificare che le misure tecniche e organizzative soddisfino i requisiti di conformità necessari.

Il titolare prende atto che, in caso di richieste di portabilità dei dati personali avanzate dai rispettivi Interessati, e solo in relazione a servizi che generino dati personali rilevanti a tal fine, il responsabile presterà assistenza al titolare mettendo a disposizione le informazioni necessarie per estrarre i dati richiesti in formato conforme a quanto previsto dalla legislazione in materia di protezione dei dati personali. Quanto sopra non è applicabile in caso di rapporti aventi ad oggetto prodotti installati presso il titolare o presso fornitori del titolare.

6.8. Funzioni e responsabilità di Joker S.r.L.

Fermo restando quanto precisato negli Allegati e, parimenti, che sono al di fuori del dominio di gestione del responsabile i servizi e le applicazioni dei sistemi e degli applicativi interamente sottoposti a gestione, controllo ed amministrazione da parte di altri fornitori o gestori esterni, al responsabile possono, in alcuni casi, essere affidate attività, funzioni e responsabilità inquadrabili, anche solo in parte, nella c.d. funzione di "Amministratore del Sistema" di cui al provvedimento dell'Autorità Garante della Protezione dei Dati Personali del 27 novembre 2008, come modificato in data 25 giugno 2009 dal Disciplinare Tecnico, rinvenibile all'indirizzo indicato in nota[1].

In tali casi, in particolare e salvo quanto precisato negli Allegati (in particolare nell'Allegato 3), il responsabile è tenuto a:

1. assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento di cui al contratto in funzione della tipologia di trattamento effettuata;
2. nell'esecuzione dei, e relativamente ai, compiti affidati, garantire l'attuazione delle misure previste dalle policy e procedure privacy aziendali che siano trasmesse dal titolare, segnalando a quest'ultimo eventuali ulteriori misure necessarie per ridurre al minimo i rischi connessi con le caratteristiche intrinseche dei sistemi informatici, di distruzione o perdita, anche accidentale, dei dati e di accesso non autorizzato agli stessi;
3. impostare, se richiesto, i sistemi informatici di collegamento verso internet e di autenticazione interna in modo che siano protetti da accessi abusivi o da utilizzi illegittimi;
4. adottare, in relazione a quanto demandato nel contratto con il titolare, gli accorgimenti necessari a evitare la perdita o la distruzione, anche solo accidentale, dei dati personali di dipendenti o equiparati, nonché dei clienti e provvedere al ricovero periodico degli stessi su copie di backup, vigilando sulle procedure attivate in struttura e assicurandone la qualità e la loro conservazione in luogo adatto e sicuro;
5. configurare, con il supporto del titolare, ove richiesto, sistemi di disaster-recovery basati sul backup dei dati anche su cloud, avendo cura di definire e applicare procedure coerenti con le politiche della società sulla conservazione e tempi di ripristino;
6. coordinare le attività operative delle risorse che operano sotto la sua autorità, nel rispetto delle mansioni affidate, per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico, vigilando, in ogni caso, su tale operato;
7. garantire l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi e agli archivi del titolare. Tali registrazioni hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste e comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi. L'operato di Joker, allorché inquadrabile quale attività di A.d.S., è sottoposto ad attività di verifica per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti di dati personali.

[1] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499

Art. 7. Ricorso a sub responsabili

Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili (Allegato 3).

Il cliente titolare, in particolare, acconsente che alcune operazioni di trattamento dati siano affidate da Joker a soggetti terzi.

In questi casi, ossia qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di 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 a questo documento. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma di questo Accordo e del Gdpr.

Su richiesta motivata del titolare del trattamento, il responsabile del trattamento fornisce copia per estratto 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 copia.

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.

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.

Art. 8 Disposizioni in materia di sicurezza

Nell'eseguire il trattamento di dati personali ai fini della prestazione dei servizi, Joker si impegna ad adottare misure tecniche e organizzative adeguate per evitare il trattamento illecito o non autorizzato, la distruzione, illecita o accidentale, il danneggiamento, la perdita l'alterazione o la divulgazione, accidentali o illecite, dei dati personali. Maggiori dettagli sono indicati nell'Allegato 3.

Questo Allegato (3) contiene misure di protezione dei dati commisurate al livello di rischio presenti con riferimento ai dati personali il cui trattamento è affidato a Joker per consentire e assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi, nonché per consentire il tempestivo ripristino degli accessi ai dati in caso di violazione di sicurezza. Il titolare da atto e accetta che, tenuto conto dello stato dell'arte, dei costi, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento dei dati personali, le procedure e le misure di sicurezza implementati da Joker S.r.L. garantiscono un livello di protezione adeguato al rischio per quanto riguarda i trattamenti alla stessa affidati.

Joker potrà aggiornare e modificare nel tempo tali misure, fermo restando che gli aggiornamenti e le modifiche non potranno comportare una riduzione del livello di sicurezza complessivo dei servizi. Di tali modifiche o aggiornamenti sarà data debita comunicazione al titolare.

Qualora il titolare richieda di adottare misure di sicurezza aggiuntive, Joker si riserva il diritto di valutarne la fattibilità e di indicare il relativo costo al titolare.

Fermo restando quanto sopra, il titolare riconosce e accetta che, nella fruizione dei servizi, rimane sua esclusiva responsabilità adottare adeguate misure di sicurezza in relazione alla fruizione dei servizi da parte del proprio personale e di coloro che sono autorizzati ad accedere ai servizi.

Allo scopo il titolare si impegna a utilizzare i servizi, i prodotti e le funzionalità di trattamento dei dati personali in modo tale da garantire un adeguato livello di protezione in relazione al rischio effettivo. Si impegna, di conseguenza, ad adottare misure idonee a proteggere le credenziali di autenticazione laddove presenti, i sistemi e i dispositivi utilizzati per accedere ai servizi e per eseguire i salvataggi e i backup necessari al fine di garantire il ripristino dei dati.

Art. 9. Obblighi del titolare cliente e limitazioni

Il titolare si impegna a impartire istruzioni conformi alla normativa e a utilizzare i servizi secondo quanto previsto dalle legislazioni applicabili e ad affidare a Joker, in generale, solo trattamenti di dati personali raccolti in conformità alle norme.

L'eventuale trattamento di categorie particolari di dati personali (art. 9 del Gdpr) o di dati relativi a condanne penali e reati (art. 10 Gdpr) sarà affidato a Joker esclusivamente previo accordo scritto tra le parti.

Fermo restando che il titolare garantisce che il trattamento dei dati effettuato mediante l'utilizzo dei servizi, dei prodotti e delle prestazioni di Joker avverrà esclusivamente in presenza di idonea base giuridica, dichiara altresì, qualora il rilascio dell'Informativa sul trattamento dei dati e l'ottenimento dell'eventuale consenso debbano avvenire per il tramite del prodotto oggetto del contratto o del servizio, di procedervi autonomamente, con esclusione di ogni responsabilità in capo a Joker; dichiara altresì, laddove tali incombenze debbano avvenire per il tramite del servizio reso da Joker, di averlo previamente valutato e ritenuto confacente.

Ferma restando la più ampia collaborazione di Joker al riguardo, il titolare dichiara altresì di essere consapevole che la gestione dei dati personali relativa alle richieste degli interessati è in capo al medesimo, e provvede di conseguenza.

Art. 10. Trasferimenti

Fermo restando quanto previsto dall'articolo precedente, 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.

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.

Articolo 11. 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 Gdpr tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

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:

- 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, (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
- nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del Gdpr devono essere indicate nella notifica del titolare del trattamento e includere almeno:
  - 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;
  - le probabili conseguenze della violazione dei dati personali;
  - 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;
- nell'adempiere, in conformità dell'articolo 34 del Gdpr 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 senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

- una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- 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 Gdpr.

Articolo 10. Inosservanza e risoluzione

Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma di questo Accordo, 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.

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, il titolare del trattamento insista sul rispetto delle istruzioni.

Articolo 11. Responsabilità

Ciascuna parte è responsabile nei confronti dell'altra per i danni che dovesse causare violando questo Accordo.

Articolo 12

Le Parti si danno reciprocamente atto di avere concordato e pattuito singolarmente tutte le disposizioni qui previste e di avere specificamente concordato i contenuti di tutti gli Allegati.

ALLEGATO 1

Elenco delle parti

Titolare Cliente	**Joker S.r.L. Responsabile**
P. Iva	02504360120
Email	info@jokersrl.it
Pec	jokersrl@pecsemplice.com
Referente	Gianpaolo Cova
Data	Marzo 2023
Firma del legale rappresentante - procuratore	

Allegato 2

Descrizione del trattamento

Voce	Descrizione
Natura e caratteristiche delle attività di trattamento demandate al responsabile	Al responsabile sono affidate le seguenti attività che comportano il trattamento di dati personali: • Responsabile di gestione dei sistemi IT; • gestione sistemi sicurezza informatica; • amministrazione e dominio della rete, ad eccezione della rete telefonica integrata, sorveglianza modem/router di connettività e dei firewall di protezione; • amministrazione e sorveglianza sistemi di gestione reti VPN; • amministrazione, gestione e sorveglianza sistemi antivirus a livello server e client; • amministrazione e gestione sistemi di backup e ripristino secondo le policy concordate; • gestione e controllo di attrezzature del dominio aziendale (server, client, dispositivi portatili, attrezzature di rete cablata e wireless; motori dei db: sistemi di videosorveglianza ove presenti. • Noleggio hardware. • Noleggio software. • Analisi esigenze e necessità aziendali, verifiche macchinari e documentazione, gestionali, sistemi e applicativi. • Sviluppo sistemi e applicativi della clientela. • Esecuzione di test, verifiche, risoluzioni anomalie. • Gestione di documentazione, dati e informazioni dei clienti.
Categorie di interessati	Lavoratori, dipendenti, agenti, consulenti, liberi professionisti del Cliente (persone fisiche) Prospect, clienti, partner commerciali e fornitori del cliente (persone fisiche)

	Dipendenti o persone di contatto di potenziali clienti, clienti, partner commerciali e fornitori del Cliente Qualsiasi altro soggetto terzo con cui il Cliente decide di comunicare tramite i Servizi. Utilizzatori e visitatori del sito o della piattaforma web. Destinatari dell'invio di comunicazioni commerciali e/o di newsletter. Partecipanti ad eventi e manifestazioni, in presenza o virtuali.
Categorie di dati personali trattati	Dati personali di tipo comune, direttamente o indirettamente identificativi. Categorie particolari di dati personali.
Finalità comunicate dal titolare del trattamento	Fornire i Servizi al Cliente; Esecuzione del Contratto, del presente DPA e/o di altri contratti stipulati da e tra le Parti; Agire in base alle istruzioni del Cliente, laddove tali istruzioni siano coerenti con i termini del Contratto; Condivisione dei Dati personali con terze parti in conformità con le istruzioni del Cliente e/o in base all'utilizzo dei Servizi da parte del Cliente (ad esempio, integrazioni tra i Servizi e qualsiasi servizio fornito da terze parti, come configurato da o per conto del Cliente per facilitare la condivisione di Dati Personali tra i Servizi e tali servizi di terze parti); Rispetto delle leggi e dei regolamenti applicabili; Operare quale: responsabile di gestione dei sistemi IT; gestione sistemi sicurezza informatica; amministrazione e dominio della rete, ad eccezione della rete telefonica integrata, sorveglianza modem/router di connettività e dei firewall di protezione; amministrazione e sorveglianza sistemi di gestione reti VPN; amministrazione, gestione e sorveglianza sistemi antivirus a livello server e client; amministrazione e gestione sistemi di backup e ripristino secondo le policy concordate; gestione e controllo di attrezzature del dominio aziendale (server, client, dispositivi portatili, attrezzature di rete cablata e wireless; motori dei db: sistemi di videosorveglianza ove presenti.
Durata del trattamento	Fatta salva qualsiasi sezione del DPA e/o dell'Accordo relativa alla durata del Trattamento e alle conseguenze della sua scadenza o risoluzione, il Responsabile tratterà i dati personali per la durata dell'Accordo e la fornitura dei servizi ai sensi dello stesso, salvo diverso accordo stipulato per iscritto.
Utilizzo di subfornitori e/o sub responsabili previsto (Nome, localizzazione, tipologia di servizio, contrattualizzazione)	Il responsabile ha stipulato specifici accordi con alcuni fornitori (sub responsabili ai fini di questo documento) per la gestione digitale di dati personali e di documenti e sistemi contenenti dati personali, per la comunicazione e trasmissioni digitali, l'archiviazione digitale, l'utilizzo di servizi IT quali cloud, hosting, assistenza e manutenzione tecnica, e per la conservazione dei file, anche di log e di altri dati personali relativi all'accesso al sistema informativo aziendale nonché per l'archiviazione di copie su banche dati specifiche. Infinity Zucchetti, Enable Microsoft, Legal logger Esprit Server ospitati in UE

Allegato 3

Misure tecniche e organizzative

Sicurezza logica

Archiviazione sicura delle informazioni

I dati gestiti da Joker S.r.L. in archiviazione sono sempre criptati con chiavi di cifratura sicure. Dietro specifico accordo contrattuale viene offerta la possibilità di utilizzare chiavi di proprietà dei clienti.

Trasmissione sicura delle informazioni

I dati trasmessi in entrata e in uscita dai sistemi gestiti da Joker S.r.L. (se in hosting) vengono criptati attraverso protocolli sicuri quali ad esempio HTTPS, SFTP, VPN secondo specifica esigenza.

Eventuali eccezioni dovranno essere segnalate dal cliente fin dalle fasi iniziali del progetto e saranno soggette a proposte di riconversione sicura da parte di Joker S.r.L..

Sicurezza della rete

Le infrastrutture su cui poggiano gli applicativi gestiti da Joker S.r.L. (se in hosting) sono progettate secondo elevati standard di sicurezza:

- Sistemi di configurazione iniziale automatici permettono di limitare rischi di errate implementazioni;
- Soluzioni di Reverse Proxy per il port forwarding del traffico verso le macchine interne;
- Sistemi di filtro delle richieste indesiderate provenienti dall'esterno;
- Sistemi di protezione per tentativi di attacco DDoS;
- Sistemi di monitoraggio, di log management e aggiornamento/applicazione di patch di sicurezza;
- Ove necessario opportune soluzioni di bilanciamento.

Sicurezza dell'infrastruttura cloud

L'infrastruttura cloud, formata dai componenti hardware e software, le reti e le strutture che eseguono i servizi è tutelata dai fornitori cloud stessi per cui Joker S.r.L. ha sottoscritto specifici accordi contrattuali vincolanti in termini di sicurezza delle informazioni e protezione dei dati personali.

Ulteriori misure attivate da Joker S.r.L.:

- misure di pseudonimizzazione e cifratura dei dati personali sono attivate dietro specifica richiesta del cliente, mediante accordo separato;
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, mediante adozione, come indicato, di procedure organizzative; specifica gestione dei profili utenti delle applicazioni; formazione dedicata e periodica del personale;
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento mediante restore periodico;
- misure di identificazione e autorizzazione dell'utente mediante mantenimento, controllo e gestione di profili utente con accesso limitato alla rete ed agli archivi cartacei;
- misure di protezione dei dati durante la trasmissione: oltre a quanto già indicato, Joker S.r.L. protegge adeguatamente le comunicazioni con la clientela;
- misure per garantire la minimizzazione dei dati mediante raccolta dei dati previsti dalla normativa vigente e per garantire la qualità dei dati;
- misure per garantire la conservazione limitata dei dati come da accordi con il cliente;
- sono altresì previste specifiche procedure organizzative interne e misure per consentire la portabilità dei dati e garantire la cancellazione, la distruzione dei file cartacei con tritadocumenti e il mantenimento dei soli dati legati ad altri obblighi di legge.

Sicurezza fisica e protezione ambientale

Sicurezza fisica e ambientale di Joker S.r.L.

I locali di Joker S.r.L., con attenzione alle aree sicure contenenti dati di tipo riservato anche di tipo personale sono difesi dalle seguenti misure di sicurezza fisiche: allarmi, muri, videosorveglianza, personale di sicurezza, sistemi antintrusione e altri dispositivi elettronici. Apposite procedure regolano le visite occasionali o regolari del personale esterno all'azienda.

Joker S.r.L. è attenta anche ai fenomeni naturali come terremoti, alluvioni, eventi metereologici o incendi che possono causare rischi per la salute dei lavoratori e l'indisponibilità delle strutture; per questo effettua regolarmente sessioni di formazione al personale, prove di evacuazione e interventi migliorativi e del controllo funzionamento degli impianti speciali di sicurezza. E' presente un impianto antincendio.

Sicurezza fisica e ambientale dell'infrastruttura cloud

I fornitori cloud controllano rigorosamente l'accesso ai data center, anche nel caso di dipendenti interni. Le terze parti hanno accesso ai data center solo se espressamente autorizzati secondo specifiche policy di accesso. Prima di creare un data center i fornitori dedicano molto tempo all'analisi delle minacce potenziali e alla progettazione, implementazione e test dei controlli per verificare che sistemi, tecnologia e persone siano in grado di reagire ai rischi. Prima di scegliere una sede, sono eseguite valutazioni ambientali e geografiche. Le posizioni dei data center sono attentamente selezionate per mitigare i rischi ambientali, come alluvioni, condizioni meteorologiche estreme e attività sismica. Le zone di disponibilità sono costruite per essere indipendenti e fisicamente separate l'una dall'altra.

Competenza e Consapevolezza

Joker S.r.L. comunica regolarmente con il proprio personale circa gli obblighi esistenti relativi alla tutela delle informazioni riservate, inclusi i dati dei clienti e sulla protezione dei dati personali. In dettaglio l'azienda si avvale dei seguenti canali di comunicazione:

- Attività di formazione annuali diversificate per area aziendale
- Attività di formazione all'atto dell'assunzione di nuovi dipendenti
- Attività di aggiornamento annuali per le figure di responsabilità
- Survey interne per misurare il livello di competenza/consapevolezza
- Newsletter interne
- Cartellonistica

Joker S.r.L. monitora costantemente le prestazioni sulle attività di formazione sulla sicurezza delle informazioni attraverso specifici Key Performance Indicators.

*

JokerSrL_DPA_ProgrSvilSistGest_01

Firmato digitalmente da: COVA CAIAZZO GIAN PAOLO
Luogo: Somma Lombardo
Data: 27/04/2023 15:13:40