Accordo sul trattamento dei dati personali tra Responsabile e Sub-Responsabile del trattamento

Tra _____ con sede in _____
P. IVA _____ - REA _____ in persona del legale rappresentate p.t. di seguito Responsabile del trattamento o semplicemente RESPONSABILE, da una parte

e

IdWeb S.r.l. con sede in viale Venturelli, 11/h – 06012 Città di Castello – PG, P. IVA 02607970544 - REA PG-228909 in persona del legale rappresentate p.t. di seguito Sub-Responsabile del trattamento, o semplicemente SUB-RESPONSABILE dall'altra.

PREMESSO CHE

- che tra le parti è stato sottoscritto un contratto per il software IdSurvey, piattaforma per la creazione e somministrazione di questionari CATI CAWI e CAPI;
- che il Sub-Responsabile gestisce la piattaforma OnCloud di IdSurvey software as a service;
- Le parti indicano il titolare del trattamento nella tabella allegata sub H. Ove venissero individuati ulteriori titolari con successivi contratti stipulati dal responsabile, la tabella potrà essere aggiornata e il presente accordo si estenderà anche ad essi.

1. OGGETTO

Le presenti pattuizioni hanno ad oggetto la disciplina delle condizioni alle quali il SUB-RESPONSABILE, per conto del Responsabile, si impegna ad effettuare le operazioni di trattamento dei dati e delle informazioni personali come definiti di seguito.
Nell'ambito dei loro rapporti contrattuali, le parti si obbligano a rispettare la normativa vigente e applicabile al trattamento dei dati personali, e in particolare il REGOLAMENTO UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, applicabile dal 25 maggio 2018, di seguito anche semplicemente Regolamento.

2. DESCRIZIONE DEI TRATTAMENTI DELEGATI AL SUB-RESPONSABILE

Il Sub-Responsabile è autorizzato a trattare per conto del Responsabile i dati personali necessari a prestare i/il servizi/io forniti/o.

Natura delle operazioni di trattamento poste in essere e tipologia di dati

Il trattamento interessa le operazioni di trattamento connesse alla attività di fornitura del software IDSurvey e le operazioni di manutenzione connesse.
In ordine ai **dati personali la cui trasmissione è implicita nell'utilizzo di protocolli di comunicazione internet**. Si tratta di dati che non vengono raccolti per essere associati a soggetti identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti (es. indirizzi IP). Tali

dati vengono trattati per il corretto funzionamento del sito web e dei servizi forniti e sono acquisiti da sistemi informatici e procedure software nel corso del loro normale esercizio.

Il Sub-Responsabile, inoltre, pur non essendo preposto ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle sue consuete attività è, in molti casi, concretamente addetto a specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. In questi casi il Sub-Responsabile opera in qualità di **"Amministratore di Sistema",** ed è tenuto altresì al rispetto delle previsioni pro tempore applicabili relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009.

Attività tecniche tipiche dell'amministratore di sistema, quali il salvataggio dei dati (backup/ recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Il presente accordo si estende a questo tipo di informazioni, il cui trattamento, nei limiti sopra descritto è del tutto accidentale ed incidentale, rispetto alle mansioni alle quali è preposto.
Le presenti pattuizioni hanno ad oggetto la disciplina delle condizioni alle quali il SUB-RESPONSABILE, per conto del Responsabile, si impegna ad effettuare le operazioni di trattamento (nella limitata accezione sopra individuata) dei dati e delle informazioni personali come definiti di seguito.

La categorie di dati che formano oggetto del trattamento sono rappresentate pertanto sia dalle categorie di dati personali che il Sub-Responsabile del trattamento tratta per rendere la prestazione, sia da quelle che potrebbero essere accessibili al Sub-Responsabile durante lo svolgimento delle prestazioni che gli sono richieste.

Segnatamente, quanto alla prima ipotesi, le categorie di dati trattati sono riassunti nella tabella che segue:

Categorie di dati personali che il Sub-Responsabile tratta per rendere la prestazione.	Barrare
Dati di connessione (log o ip)	√
Credenziali di accesso	√

Quanto alla seconda ipotesi, ovvero alle tipologie di che potrebbero essere accessibili al Sub-Responsabile durante lo svolgimento delle prestazioni che gli sono richieste, le categorie di dati sono quelle di seguito specificate dal Responsabile barrando la casella corrispondente alla tipologia di trattamento:

Tipologie di dati che potrebbero essere accessibili al Sub-Responsabile durante lo svolgimento delle prestazioni che gli sono richieste.	Barrare
Dati comuni (Nome, cognome, ecc…)	√
Particolari categorie di dati (Dati sensibili, biometrici e genetici)	
Dati relativi a decisioni automatizzate	

Categorie di dati personali cui il Sub-Responsabile potrebbe accedere nell'esecuzione delle prestazioni richieste.	Barrare
Dati identificativi (nome e cognome)	
Dati anagrafici (data di nascita, luogo di nascita indirizzo, residenza)	
Dati di contatto (numero di tel. fisso o cell., email, indirizzo per posta cartacea)	
Informazioni demografiche (genere, età)	
Dati dei documenti di identità (n. carta di identità o fotocopia)	
Curricula	
Dati relativi alla geolocalizzazione	
Altro	

Ove siano trattate categorie particolari di dati ai quali il Sub-Responsabile potrebbe incidentalmente accedere nella esecuzione delle prestazioni il Responsabile dovrà indicarlo barrando le caselle indicate nella tabella che segue:

Categorie particolari di dati personali cui il Sub-Responsabile potrebbe accedere nell'esecuzione delle prestazioni richieste	Barrare
Dati giudiziari relativi a condanne penali	
Dati relativi alla salute	
Dati che rivelano l'origine razziale o etnica	
Dati che rivelano le opinioni politiche	
Dati che che rivelano convinzioni religiose o filosofiche	
Dati dati che rivelano l'appartenenza sindacale	
Dati genetici	
Dati biometrici	
Dati relativi alla vita sessuale	
Dati relativi all'orientamento sessuale	

Anche al fine di evidenziare la presenza di categorie di persone vulnerabili, il responsabile dichiara che i dati riguardano le seguenti categorie di interessati: _____

_____

3. DURATA DELL'ACCORDO

Il presente accordo avrà durata pari a quella della durata del servizio aderito e descritto in premessa. Il presente accordo entrerà in vigore tra le parti dalla sottoscrizione di entrambe, nel caso di sottoscrizione asincrona, al momento dell'ultima sottoscrizione.

4. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL SUB-RESPONSABILE

Il Responsabile del trattamento si obbliga a:

- fornire al Sub-Responsabile del trattamento dei dati personali di cui al n. II del presente accordo;
- documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Sub-Responsabile;
- assicurare, sin d'ora e per tutta la durata del trattamento, il rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del Sub-Responsabile;
- supervisionare il trattamento, compresa la realizzazione degli audit e le ispezioni col contributo del Sub-Responsabile.

5. OBBLIGHI DEL SUB-RESPONSABILE

Il Sub-Responsabile si impegna innanzi al Responsabile a:

- trattare i dati personali per le sole **finalità** oggetto del trattamento;
- trattare i dati personali in conformità alle **istruzioni scritte** del Responsabile, allegate al presente contratto; se il Sub-Responsabile ritiene che un'istruzione ricevuta dal Responsabile rappresenti una violazione del Regolamento generale sulla protezione dei dati, o del diritto dell'Unione europea o del diritto di uno Stato membro, egli informa tempestivamente il Responsabile del trattamento. Inoltre, se il Sub-Responsabile è tenuto a procedere a un trasferimento di dati verso un paese terzo o un'organizzazione internazionale in virtù del diritto dell'Unione o del diritto di uno Stato membro al quale è sottoposto, egli deve informare il Responsabile del trattamento di tale obbligo giuridico prima del trattamento a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- **garantire la riservatezza** dei dati personali trattati nell'ambito del presente contratto;
- assicurare che le **persone autorizzate** a trattare i dati a carattere personale in virtù del presente contratto:
    - si impegnino a rispettare la riservatezza o siano sottoposte a un idoneo obbligo legale di riservatezza;
    - ricevano le istruzioni necessarie a mantenere la protezione dei dati a carattere personale.
- Tengano conto, per quanto riguarda strumenti, prodotti, applicazioni o servizi, dei principi della privacy sin dalla progettazione (privacy by design) e della privacy per impostazione predefinita (privacy by default);
- il Sub-Responsabile non si oppone a che una copia del presente accordo sia trasmessa dal Responsabile al Titolare del trattamento, per consentirgli il controllo del rispetto delle istruzioni e degli obblighi imposti al Responsabile del trattamento con pregresso accordo, ma non sarà necessario mettere a disposizione del Titolare del trattamento le clausole relative a questioni commerciali che non incidono sul contenuto giuridico della protezione dei dati dell'accordo con il Sub-Responsabile.
- il Sub-Responsabile si obbliga in caso di fallimento del Responsabile del trattamento (o altra causa che comporti la perdita della sua capacità di agire), a riconoscere al Titolare del trattamento il diritto di ordinare al Sub-Responsabile la restituzione o la cancellazione dei dati personali che il Responsabile (e di conseguenza il Sub-Responsabile) trattavano per suo conto, secondo quanto previsto di seguito in ordine alla "sorte dei dati".

6. SUBRESPONSABILI - AUTORIZZAZIONE GENERALE

IdWeb può ricorrere a un altro Sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento. In questo caso egli informa preventivamente e per iscritto il responsabile di tutte le modifiche riguardanti l'aggiunta o la sostituzione dei Sub-Responsabili. Tali informazioni devono indicare chiaramente le attività di trattamento effettuate dall'altro Sub-Subresponsabile, l'identità e i recapiti dell'altro subresponsabile, e la data del contratto relativo al sub-trattamento. Il responsabile del trattamento dispone di un periodo di 15 giorni a far data dal ricevimento delle informazioni per presentare le proprie obiezioni. Il sub trattamento non può avere inizio sino a che il termine indicato non sia spirato senza che il responsabile abbia presentato obiezioni.

Il Sub-Contraente di IdWeb sarà tenuto a rispettare gli obblighi del presente contratto per conto e secondo le istruzioni del responsabile del trattamento. E' compito di IdWeb assicurare che l'altro Sub-Contraente che egli abbia individuato presenti le medesime garanzie sufficienti in ordine alla messa in atto delle misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento Generale sulla protezione dei dati.
Se il nuovo responsabile (Sub-Contraente) individuato da IdWeb omette di adempiere i suoi obblighi in materia di protezione dei dati, IdWeb conserva nei confronti del Responsabile la piena responsabilità per l'adempimento degli obblighi del suo Sub-Contraente ("Sub-Subresponsabile").

7. DIRITTO DEGLI INTERESSATI ALL'INFORMATIVA

E' compito del Responsabile del trattamento fornire l'informativa agli interessati del trattamento al momento in cui i dati sono raccolti.

8. ESERCIZIO DEI DIRITTI DA PARTE DEGLI INTERESSATI

Nella misura del possibile il Sub-Responsabile del trattamento deve aiutare il Responsabile del trattamento (ed il Titolare per cui conto il responsabile opera) ad adempiere ai propri obblighi di fornire riscontro alle richieste degli interessati in ordine al diritto d'accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a opporsi a una decisione individuale automatizzata (compresa la profilazione).
Quando gli interessati si rivolgano al Sub-Responsabile per l'esercizio dei loro diritti, il Sub-Responsabile deve inviare queste richieste, non appena vengono ricevute, per posta elettronica all'indirizzo di posta elettronica indicato in calce al presente accordo (allegato B). Ove il Responsabile non provveda a tale incombente il Sub-Responsabile è libero da ogni obbligo.

9. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI

Il Sub-Responsabile comunica al Responsabile del trattamento tutte le violazioni di dati a carattere personale nel **termine massimo di 48 ore** dal momento in cui è venuto a conoscenza della violazione, con le seguenti modalità: comunicazione all'indirizzo di posta elettronica indicato nell'allegato B al presente contratto.
Tale comunicazione è accompagnata dalla notizia della messa a disposizione (ove possibile) di tutta la documentazione utile (la cui modalità di trasmissione verrà concordata tra le parti) al fine di permettere al Responsabile del trattamento, di provvedere, se necessario, alla notifica di tale violazione all'Autorità di Controllo competente nei termini di legge.

10. AUSILIO DEL SUB-RESPONSABILE PER IL RISPETTO, DA PARTE DEL RESPONSABILE, DEGLI OBBLIGHI GRAVANTI SUL RESPONSABILE STESSO, FORNENDO LE INFORMAZIONI IN SUO POSSESSO.

Il Sub-Responsabile aiuta il Responsabile del trattamento nell'effettuazione della valutazione di impatto sulla protezione dei dati personali.

Il Sub-Responsabile del trattamento aiuta il Responsabile del trattamento nell'effettuazione della consultazione preventiva rivolta all'Autorità di controllo.

11.MISURE DI SICUREZZA

Il Sub-Responsabile si obbliga, ai sensi dell'articolo 32, a mettere in atto le misure di sicurezza descritte nell'allegato "IdSurvey infrastruttura on Cloud" che il Responsabile dichiara adeguate e conformi alle istruzioni da impartire.
Il Responsabile delega al Sub-Responsabile l'adozione di misure diverse rispetto a quelle descritte nell'allegato "IdSurvey infrastruttura on Cloud" a condizione che il Sub-Responsabile rispetti i parametri definiti dall'articolo 32 del Regolamento. Il Sub-Responsabile, valutato il rischio e qualora lo ritenga necessario anche in considerazione dei costi e dello stato dell'arte si obbliga a mettere in atto le misure di sicurezza seguenti, se applicabili e congrue:

- la pseudonimizzazione e la cifratura dei dati personali;
- misure che abbiano la capacità di assicurare su base permanente la riservatezza;
- l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- misure che abbiano la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre, per quanto concerne i trattamenti effettuati per fornire il Servizio dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Sub-Responsabile è tenuto altresì al rispetto delle previsioni pro tempore applicabili relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009. Il Sub-Responsabile, in particolare, si impegna ad attribuire le funzioni di amministratore di sistema solo previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Si impegna altresì a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Responsabile su richiesta del medesimo.
Si impegna, infine, ad adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

12.SORTE DEI DATI

Al termine della prestazione del servizio relativo al trattamento dei dati il Sub-Responsabile si obbliga a restituire tramite download dei dati direttamente dal software e per un periodo di 30 giorni, tutti i dati personali al Responsabile del trattamento, salvo che questi gli ordini di distruggerli.
La restituzione si accompagna alla distruzione di tutte le copie esistenti nel sistema informatico del Sub-Responsabile.

13. SUB-RESPONSABILE PER LA PROTEZIONE DEI DATI (DATA PROTECTION OFFICER, DPO O RPD)

Il Sub-Responsabile del trattamento non è obbligato alla nomina del Sub-Responsabile per la protezione dei dati (DPO o RPD). Si impegna comunque a comunicare al Responsabile il nome e i recapiti del Sub-Responsabile per la protezione dei dati ove ne nominasse uno.

14. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Sub-Responsabile dichiara di tenere per iscritto un registro di tutte le attività di trattamento effettuate per conto del Responsabile comprendente tutti gli elementi elencati a tal fine dall'articolo 30 del Regolamento.

15. DOCUMENTAZIONE

Il Sub-Responsabile mette a disposizione del Responsabile del trattamento la documentazione necessaria a dimostrare il rispetto di tutti i suoi obblighi, e per consentire gli audit, comprese le ispezioni, al Responsabile del trattamento o altro soggetto da questi a tal fine incaricato, e contribuire agli audit.

16. CLAUSOLE FINALI

Le premesse e gli allegati fanno parte integrante del presente accordo.
Con la sottoscrizione del presente accordo, il Responsabile del trattamento, fermo restando quanto previsto dal Regolamento (UE) 2016/679 e nel rispetto delle istruzioni ricevute dal Titolare del trattamento e dei principi di responsabilizzazione e controllo, prende atto che, nel rispetto del presente accordo e in particolare di quanto disposto dal punto 5, e limitatamente al servizio oggetto del presente accordo, qualora il Sub-Responsabile del trattamento si avvalga di un ulteriore sub-responsabile che trasferisca i dati verso Paesi terzi, potrà proporre l'adozione delle Clausole Contrattuali Standard di cui alla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021, esclusivamente con riferimento ai moduli pertinenti, ossia da responsabile a responsabile (P2P) e da responsabile del trattamento a titolare (P2C), nonché delle eventuali misure contrattuali supplementari che le accompagnino.

L'efficacia di tali Clausole, nonché delle relative misure contrattuali supplementari, resta in ogni caso subordinata al rispetto delle istruzioni ricevute dal Titolare del trattamento e, ove necessario, alla preventiva approvazione scritta del Titolare stesso.

Il presente accordo costituisce esecuzione del rinvio operato dalle clausole “riservatezza e privacy” contenute nel contratto IdSurvey e supera e sostituisce per intero ogni atto ovvero accordo scritto o verbale intervenuto tra le parti che regola la medesima materia e il medesimo oggetto ivi disciplinati.

17. FORO COMPETENTE

Le Parti dichiarano che per ogni controversia relativa all'interpretazione, alla esecuzione ed alla risoluzione del presente Contratto sarà esclusivamente competente il Tribunale di Perugia.

18. LEGGE APPLICABILE

Per quanto non espressamente previsto nel presente Contratto, le Parti fanno espresso rinvio alle norme della legge italiana vigenti al momento della sua conclusione che regolano casi simili o materie analoghe.

Luogo _____ data _____

Il Responsabile _____ Il Sub-Responsabile _____

Ai sensi e per gli effetti degli artt. 1341 e 1342 il Responsabile dichiara di approvare espressamente le clausole nn 16 (le clausole tipo e le misure contrattuali supplementari), 17 (foro competente) e 18 (Legge applicabile)

Luogo _____ data _____

Il Responsabile _____

Allegato A

Nominativo del DPO del Responsabile (se applicabile)	Dati di contatto

Allegato B - Recapiti

Recapiti del Responsabile per le comunicazioni previste nel presente accordo

Evento	Dati di contatto
Data Breach	
Istanze di accesso	
Autorità Garante o Altra Autorità	

Recapiti del Sub-Responsabile per le comunicazioni previste nel presente accordo

Evento	Dati di contatto
Data Breach	Andrea Martinelli - andrea.martinelli@idweb.it
Istanze di accesso	Andrea Martinelli - andrea.martinelli@idweb.it
Autorità Garante o Altra Autorità	Andrea Martinelli - andrea.martinelli@idweb.it

Allegato C

“Sub-responsabili”
Il Sub-Responsabile è autorizzato a sub-appaltare parte delle operazioni di trattamento ai seguenti Sub-Responsabili (siano essi o meno appartenenti al Gruppo del Sub-Responsabile).

La seguente tabella mappa i sub-responsabili ingaggiati dal Sub-Responsabile.

Paese in cui è stabilito il Responsabile	**Sub-Responsabile**	**Sub-responsabili**
	Italia	Italia, Francia, Danimarca e Stati uniti.

Subresponsabile	**Dati di contatto**	**DPO**	**Utilizzato per**
AD CONSULTING S.p.A	Via Pier Paolo Pasolini n.15 41123 Modena (MO) P. IVA/C.F. 03410070365	dpo@adcgroup.com	Azure Cloud
The Rocket Science Group , LLC	Sede Legale: 675 Ponce de Leon Ave. NE, Atlanta, Georgia 30308, US .	dpo@mailchimp.com	Email-Sender
ONLINECITY.IO ApS VAT. no. DK27364276	Buchwaldsgade 50 - 5000 Odense C - Danmark • Tel (+45) 6611 8311 • e-mail tinfo@onlinecity.io	N.A.	SMS-Sender
OpenAI OpCo, LLC	1455 3rd Street, San Francisco, CA 94158	privacy@openai.com	Funzionalità AI: Codifica risposte AI Analisi, report Insight AI e domande Follow-UP

I dati extra UE vengono trasferiti soltanto nel caso in cui il Titolare o Responsabile utilizzi il sistema di invio email integrato in IdSurvey (EmailSender) e si limitano esclusivamente all'indirizzo email del destinatario e al contenuto del messaggio. Eventuali dati personali inseriti dal Titolare o Responsabile nel testo dell'email saranno trasferiti unitamente al messaggio, in quanto necessari alla relativa trasmissione.

Funzionalità di Intelligenza Artificiale
Le funzionalità di Intelligenza Artificiale sono parte integrante della piattaforma IdSurvey. Il loro utilizzo è rimesso esclusivamente alla scelta del Titolare o Responsabile del trattamento o degli utenti da esso autorizzati. Qualora tali funzionalità non vengano utilizzate, nessun dato è trasmesso ai relativi fornitori di servizi AI.

Nell'ambito delle funzionalità di Intelligenza Artificiale vengono trasmessi esclusivamente i dati strettamente necessari all'elaborazione richiesta, quali, a titolo esemplificativo, il testo della domanda, il contesto necessario all'elaborazione, le istruzioni operative (prompt) generate dal sistema e i contenuti testuali forniti dagli interessati (ad esempio risposte aperte o conversazioni di follow-up). Non vengono trasmessi ulteriori dati del progetto o dati identificativi degli interessati, salvo che tali informazioni siano direttamente contenute nei testi inseriti dagli utenti o dagli interessati.

Restano esclusi i servizi non forniti dal Sub-Responsabile e soggetti a separati accordi tra il Responsabile e il Sub-Responsabile.

La tabella dei sub-responsabili verrà aggiornata di volta in volta e il Responsabile verrà notificato di conseguenza in modo che possa opporsi all'impiego di nuovi sub-responsabili

Allegato D

Modello per la comunicazione della violazione dei dati dal Sub-Responsabile al Responsabile (ai fini del c.d. "data breach")

REPORT DELLA VIOLAZIONE

Parte 1: avviso di violazione	**Da compilare a cura di chi ha scoperto la violazione**
Data della scoperta della violazione:	
Data della violazione:	
Dove si è verificata la violazione? Denominazione e descrizione della banca dati o dello strumento (computer rete, pc portatile, tablet, chiavetta usb altra memoria rimovibile, disco esterno, file o parte di un file, strumento di backup, documento cartaceo o altro -specificare)	
Ubicazione dello strumento o banca dati:	
Nome della persona che ha scoperto la violazione:	
Contatti della persona che ha scoperto la violazione:	
Breve descrizione della violazione: • lettura (presumibilmente i dati non sono stati copiati); • copia (i dati sono ancora presenti sui sistemi del Responsabile); • alterazione (i dati sono presenti sui sistemi ma sono stati alterati); • cancellazione (i dati non sono più sui sistemi del Responsabile e non li ha neppure l'autore della violazione); • furto (i dati non sono più sui sistemi del Responsabile e li ha l'autore della violazione); • altro (specificare).	
Numero di interessati coinvolti: (prima stima approssimativa; se è possibile determinarlo, nel caso coinvolga tutti gli interessati, specificarlo; specificare altresì se non è possibile determinare il numero e se il numero presumibilmente resterà ignoto)	
La violazione costituisce un rischio per gli interessati? (descrivere brevemente se si ritiene che comporti un rischio)	
Breve descrizione delle azioni già intraprese per mitigare il rischio:	

	Da compilare a cura del ricevente
Ricevuto da:	
Data:	
Prossime azioni (notifica comunicazione):	
Entro il:	

Parte 2: valutazione del rischio	**Da compilare a cura del soggetto competente a effettuare la valutazione**
Descrizione dei sistemi IT, degli strumenti, dei device degli archivi coinvolti nella violazione:	
Misure tecniche e organizzative applicate ai dati:	
Descrizione dell'evento: • perdita; • indisponibilità; • lettura (presumibilmente i dati non sono stati copiati); • copia (i dati sono ancora presenti sui sistemi del Responsabile); • alterazione (i dati sono presenti sui sistemi ma sono stati alterati); • cancellazione (i dati non sono più sui sistemi del Responsabile e non li ha neppure l'autore della violazione); • furto (i dati non sono più sui sistemi del Responsabile e li ha l'autore della violazione); • accesso esterno non autorizzato; • accesso interno non autorizzato; • errore; • fenomeno naturale (incendio, inondazione ecc.); • altro (specificare).	
Qual è la natura delle informazioni interessate dalla violazione? (copia informatica di documenti cartacei, documenti informatici, documenti cartacei)	
Quanti dati sono interessati? Es. Hanno rubato una banca dati con 1000 indirizzi IP, non si conosce a quanti utenti appartengono. Non va necessariamente specificato un numero: se viene violata una banca dati di cartelle cliniche i dati saranno "molti", anche se riferiti a pochi pazienti. In caso di perdita o furto di laptop o altro device, quando era stato fatto l'ultimo backup disponibile?	
Si tratta di informazioni uniche? Questa violazione può comportare conseguenze finanziarie legali danni all'immagine o reputazioni al Responsabile o al Sub-Responsabile o agli interessati o ad altre terze parti se resa nota?	
Quanti interessati coinvolge la violazione?	

Sono coinvolte particolari categorie di dati o altri dati ad alto rischio? (indicare le categorie coinvolte) Categorie: dati anagrafici/codice fiscale; dati di accesso e di identificazione (user name, password, customer ID, altro); Dati ad alto rischio che rivelano: • l'origine razziale o etnica; • le opinioni politiche; • le convinzioni religiose o filosofiche; • l'appartenenza sindacale; • dati relativi allo stato di salute; • dati relativi alla vita sessuale o all'orientamento sessuale; • dati genetici; • biometrici; • dati relativi a reati o condanne penale.	
Tipologia di interessati: • candidati; • dipendenti; • dipendenti dei partner commerciali (e.g. dealer, fornitori, etc..); • clienti (inclusi i prospects). Attenzione in particolare a: • informazioni personali relative a categorie particolarmente vulnerabili o relative a minori; • informazioni particolari relative ai lavoratori, come ad esempio test attitudinali, buste paga ecc.; • whistleblower.	
Conseguenze ipotizzabili: A) provocare danni fisici, materiali o immateriali alle persone fisiche (ad esempio informazioni che possono compromettere la sicurezza degli interessati se rese note); B) furti di identità o usurpazioni (informazioni che possono essere utilizzate per competere furti di identità o altri reati come ad esempio account bancari o altre informazioni finanziare e identificative come ad esempio copie di carte di identità e passaporti o altri documenti di riconoscimento); C) perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti; D) discriminazione (esempio dati sulla etnia, razza religione convinzioni filosofiche orientamento sessuale, talvolta appartenenza sindacale); E) perdite finanziarie; F) de-cifratura non autorizzata della pseudonimizzazione (es. whistleblowing); G) pregiudizio alla reputazione; H) perdita di riservatezza dei dati personali protetti da segreto professionale; I) qualsiasi altro danno economico o sociale significativo alla persona fisica interessata; J) grave disagio e stress se le informazioni vengono rese note o divulgate; K) informazioni relative all'identità di individui che si sono avvalsi di procedure di whistleblowing e causare ritorsioni compromettere indagini.	
la violazione è localizzata o generalizzata all'intero sistema?	

E’ possibile superare l’incidente che ha provocato la violazione con le normali operazioni di ripristino?	
In alternativa, è necessario l'intervento di soggetti esterni?	
La violazione è solo temporanea o è permanente?	

Parte 3: azioni intraprese	**Da compilarsi a cura del soggetto competente**
Data:	
Annotazione nel registro /n. violazione:	
Quante registrazioni di dati personali sono state colpite dalla violazione dei dati personali? Indicare numero approssimativo • da 1 a 100; • da 100 a 1000; • da 1000 a 10.000; • da 10.000 a 100.000; • da 100.000 a 500.000; • da 500.000 a 1.000.000; • oltre 1.000.000;	
Azioni intraprese - Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?	
Quali misure tecnologiche e organizzative sono state adottate (o ci si propone di adottare) per attenuare i possibili effetti negativi della violazione?	
Follow up.	
Occorre procedere alla notifica all'Autorità territoriale competente:	sì/no
Occorre dare comunicazione agli interessati:	sì/no (dettagli)
La violazione potrebbe riguardare: A) informazioni che possono compromettere la sicurezza degli interessati se rese note; B) informazioni che possono comportare discriminazione se rese note C) informative relative a minori o soggetti deboli; D) informazioni che se diffuse arrecano pregiudizio alla reputazione; E) informazioni che possono causare grave disagio o stress se rese note.	

Allegato E

Istruzioni generali impartite dal Responsabile al Sub-Responsabile del Trattamento

Il Sub-Responsabile, sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate, oltre agli ulteriori obblighi previsti nel suesteso accordo, e dunque dovrà:

- tenere un registro, come previsto dall'art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Società, contenente:
    - il nome e i dati di contatto del Sub-Responsabile e del Responsabile e, laddove applicabile, del Sub-Responsabile della protezione dei dati;
    - le categorie dei trattamenti effettuati per conto del Responsabile;
    - ove applicabile, i trasferimenti di dati personali verso un paese non appartenente all'Unione Europea, compresa l'identificazione di tale paese e, per i trasferimenti di cui al secondo comma dell'art. 49 del GDPR, la documentazione delle garanzie adeguate;
    - ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate;
- organizzare le strutture, gli uffici e le competenze necessarie e idonee a garantire il corretto adempimento del contratto;
- astenersi dal contattare per finalità diverse dall'incarico i nominativi trattati attraverso il servizio;
- non diffondere o comunicare a terzi le informazioni, ivi inclusi i dati personali trattati per rendere il Servizio;
- provvedere ad individuare per iscritto i soggetti autorizzati al trattamento ai sensi della Normativa applicabile e impartire a questi ultimi specifiche e dettagliate istruzioni dirette ad assicurare il pieno rispetto delle disposizioni di cui alla Normativa applicabile;
- adottare le misure tecniche ed organizzative di sicurezza, previste dall'allegato "IdSurvey infrastruttura on Cloud";
- **avvisare il Responsabile del trattamento, di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria eventualmente ricevuta inviando copia delle istanze all'indirizzo e-mail indicato dal Responsabile per concordare congiuntamente il riscontro; Il Responsabile verrà altresì tempestivamente avvisato di ogni informazione trasmessa dai subresponsabili in ordine a richieste di accesso governative da parte di autorità o agenzie o servizi di Paesi terzi;**
- mantenere un costante aggiornamento sulle prescrizioni di legge in materia di trattamento dei dati personali, nonché sull'evoluzione tecnologica di strumenti e dispositivi di sicurezza, modalità di utilizzo e relativi criteri organizzativi adottabili;
- garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali non coerente con gli specifici trattamenti svolti in adempimento dell'incarico medesimo;
- Rispettare le istruzioni impartite dal responsabile del trattamento attraverso il pannello di controllo di IdSurvey, in relazione a download dei dati (portabilità), cancellazione, copia, generazione di profili di autenticazione e permessi, ecc. che si intendono come "istruzioni scritte" ai sensi del presente accordo.

ALLEGATO F
informazioni sui trattamenti effettuati all'estero

Servizio	Sub-Responsabile	Paese terzo in cui vengono trasferiti i dati	Misura di salvaguardia
Mailchimp	The Rocket Science Group , LLC	USA	SCC in Data Processing Addendum
Servizi AI	OpenAI OpCo, LLC	USA	Standard Contractual Clauses (SCC) nel Data Processing Addendum (DPA)

In ordine a quanto disposto dal punto 5 dell'**Accordo sul trattamento dei dati personali tra responsabile e sub-responsabile del trattamento, il Responsabile si considera informato dei trasferimenti effettuati in Paesi terzi come descritti nel presente allegato.**

I dati extra UE vengono trasferiti soltanto nel caso in cui il Titolare o Responsabile utilizzi il sistema di invio email integrato in IdSurvey (EmailSender) e si limita esclusivamente all'indirizzo email e al testo della mail stessa. Nell'ambito delle funzionalità di Intelligenza Artificiale vengono trasmessi esclusivamente i dati strettamente necessari all'elaborazione richiesta, quali, a titolo esemplificativo, il testo della domanda, il contesto necessario all'elaborazione, le istruzioni operative (prompt) generate dal sistema e i contenuti testuali forniti dagli interessati (ad esempio risposte aperte o conversazioni di follow-up).

Non vengono trasmessi ulteriori dati del progetto o dati identificativi degli interessati, salvo che tali informazioni siano direttamente contenute nei testi inseriti dagli utenti o dagli interessati.

ALLEGATO G

IdSurvey infrastruttura OnCloud

Da 20 anni ospitiamo i dati dei clienti prestando la massima attenzione alla loro protezione. Per assicurare il più alto grado di sicurezza possibile, utilizziamo dispositivi efficaci e adottiamo una serie di best practice a tutti i livelli della nostra organizzazione e delle infrastrutture.



Sicurezza datacenter:

- data center conformi agli standard di settore, ad esempio ISO/IEC 27001:2013 e NIST SP 800-53, per la sicurezza e l'affidabilità.
- Accesso fisico ai server limitato al personale accreditato.
- Accesso ai datacenter consentito esclusivamente tramite sistemi di autenticazione multifattore per il personale accreditato.
- Sorveglianza video e umana 24/7.
- Sale dotate di sistemi di rilevamento di particelle di fumo e soppressione incendi.
- Personale tecnico presente 24 ore su 24, 7 giorni su 7.
- Data center dotati di sistemi di alimentazione ridondanti, inclusi UPS e gruppi elettrogeni, per garantire continuità del servizio in caso di interruzioni della rete elettrica.
- Microsoft Azure è conforme a un ampio ventaglio di standard internazionali (ISO/IEC 27018, SOC 1/2/3, GDPR, CSA STAR, ecc.), garantendo il rispetto delle normative in materia di protezione dei dati.

Sicurezza e caratteristiche

- Infrastruttura Microsoft Azure basata su tecnologia Hyper-V e servizi cloud nativi, con aggiornamenti e patch di sicurezza automatici inclusi.
- Connettività ad alte prestazioni grazie alla rete globale Microsoft, con disponibilità di ampia larghezza di banda.
- Supporto di reti virtuali isolate (Azure Virtual Network) con gestione sicura e scalabile delle subnet.
- Supporto Microsoft per incidenti 24/7/365.
- Portale Azure e API per la gestione delle risorse cloud.
- Strumenti integrati per il testing di resilienza e la verifica della continuità operativa.
- Servizi di monitoraggio avanzato tramite Azure Monitor e Application Insights.
- Gestione automatizzata dell'infrastruttura host con aggiornamenti e manutenzione trasparenti.
- Scalabilità on-demand delle risorse con provisioning rapido.
- Deploy automatico.
- Local Redundancy Storage.
- Sistema basato su standard Microsoft Azure riconosciuti a livello internazionale.
- SSL
- Backup tramite Azure Backup e soluzioni ridondate.
- Firewall e rete: Azure Firewall, Network Security Groups e protezioni a livello di rete.

Protezione Anti-DDoS PRO

Con la crescita esponenziale del volume di dati online, gli attacchi distribuiti per l'interruzione del servizio (DDoS, Distributed Denial of Service) sono sempre più frequenti.

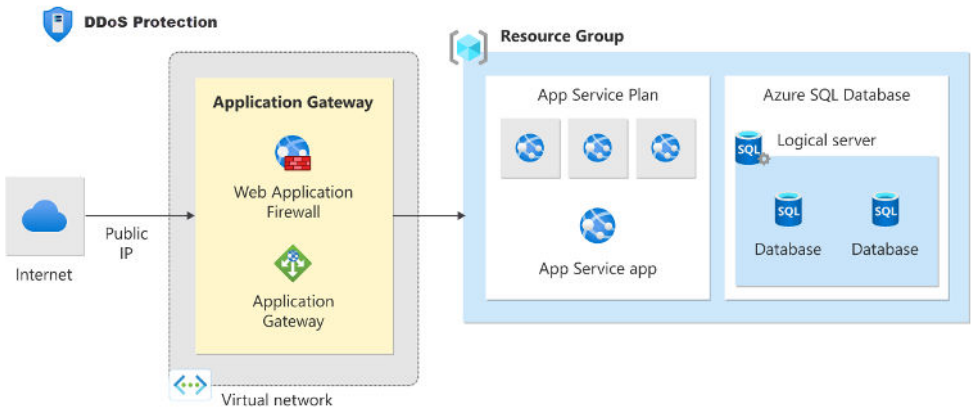
Un attacco DDoS ha l'obiettivo di rendere indisponibili server, applicazioni o intere infrastrutture, sovraccaricando la larghezza di banda o esaurendo le risorse di calcolo fino a bloccarne la capacità di risposta.

Per garantire la continuità del servizio, Microsoft Azure integra DDoS Protection.

La protezione si basa su tecniche di mitigazione automatiche che consentono di:

- analizzare in tempo reale e ad alta velocità il traffico di rete,
- identificare e deviare il traffico malevolo prima che raggiunga le risorse,
- filtrare i pacchetti non legittimi e consentire solo il traffico valido.

Questa protezione è attiva 24/7 e sfrutta la rete globale Microsoft per garantire resilienza anche contro attacchi su larga scala.



Certificazioni struttura server farm OnCloud

Il servizio Cloud è progettato e sviluppato secondo i più rigorosi standard di sicurezza internazionali, con un approccio Security by Design e Defense in Depth, che garantisce il massimo livello di protezione dei dati.

Microsoft Azure adotta un approccio trasparente e sottoposto a regolari processi di audit indipendenti. I sistemi di gestione della sicurezza sono certificati secondo ISO/IEC 27001 e conformi a numerosi altri standard, tra cui:

- ISO/IEC 27017 (controlli di sicurezza specifici per il cloud),
- ISO/IEC 27018 (protezione dei dati personali nel cloud),
- SOC 1, SOC 2 e SOC 3,
- PCI DSS (sicurezza dei dati di pagamento),
- CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry),
- GDPR compliance per la protezione dei dati personali,
- FedRAMP e HIPAA per specifici requisiti normativi internazionali.

L'elenco aggiornato e completo delle certificazioni è disponibile qui: https://learn.microsoft.com/en-us/azure/compliance/

ALLEGATO H
Titolari del trattamento

Titolare	Dati di contatto	DPO (dati di contatto del DPO)