EURO PRIVACY

GDPR 679/2016

.....

.....



24/05/19	0	Emissione	Angelo Lissoni
DATA	**REV**	**OGGETTO**	**APPROVAZIONE**

INDICE

1. IL CONTESTO 2
2. DEFINIZIONI 4
3. FAQ 7
4. ATTIVITÀ DELL'ASSOCIAZIONE E DATI DEL TITOLARE 10
5. ORGANIGRAMMA 10
6. ASSET 10
7. TRATTAMENTI 11
7.1 GESTIONE CONCORSO 11
7.2 GESTIONE EDITORIA 12
7.3 AREA LEGALE 13
7.4 SICUREZZA SUI LUOGHI DI LAVORO 13
7.5 AREA FORMAZIONE 14
7.6 ADEMPIMENTI CIVILISTICO-FISCALI 15
7.7 AREA PRIVACY 16
8. VALUTAZIONE D'IMPATTO (DPIA) 16
9. AUDIT 17
10. DATA BREACH 18

1. IL CONTESTO

L'Internet degli Oggetti è l'estensione di Internet al mondo degli oggetti e dei luoghi. Attraverso chip e sensori gli oggetti possono interagire tra loro e con la realtà circostante. Il mondo fisico, a tendere, può essere digitalizzato, monitorato e virtualizzato. Secondo Gartner, l'IT è uno degli elementi disruptive per molti comparti industriali e Capgemini stima che tra 5 anni il 33% della popolazione mondiale indosserà almeno un Wearableo Fitness Device, il 20% degli autoveicoli sarà dotato di dispositivi connessi mentre nel 38% delle nostre case sarà presente almeno uno tra sensori per la sicurezza, sensori bianchi o robot per la pulizia.

Secondo un'indagine d Maggio 2017, portata avanti dal Global Privacy Enforcement Network (Gpen), di cui fa parte anche il Garante italiano, per verificare il rispetto della privacy nell'IT:

1) Il 59% degli apparecchi non offre informazioni adeguate su come i dati personali degli interessati sono raccolti, utilizzati e comunicati a terzi;
2) il 68% non fornisce appropriate informazioni sulle modalità di conservazione dei dati;
3) il 72% non spiega agli utenti come cancellare i dati dal dispositivo;
4) il 38% non garantisce semplici modalità di contatto ai clienti che desiderano chiarimenti in merito al rispetto della propria privacy.

Poiché nel 2020 ci potrebbero essere circa 30 miliardi di dispositivi connessi a Internet, si comprende come il problema più grande di quest'epoca elettronica riguardi la privacy. In effetti sempre più il modo di comunicare, conoscere ed apprendere si sta digitalizzando ed il nostro essere parte della società spesso si configura o meglio si confonde con l'esser connessi, presenti e visibili sui social-network, o comunque sul web. La "visibilità" digitale presenta un confine molto labile tra ciò che vogliamo sia pubblico e ciò che non riusciamo a mantenere "privato". Per fortuna, questo non vale per tutte le persone e non vale in tutte le parti del nostro mondo sempre più globalizzato, ma il trend delle nostre società occidentali appare segnato da un avanzare della tecnologia estremamente più veloce della capacità degli uomini di adeguarsi ai nuovi strumenti ed alle nuove idee e possibilità che queste offrono, soprattutto per quanto riguarda la capacità di cogliere i rischi che queste novità portano con loro. L'ignoranza verso il tecnologicamente nuovo, intesa come non-conoscenza e cioè ignorare cosa significa o cosa comporta l'uso di una nuova App o di un nuovo Social, espone tutti noi a pericoli o rischi assolutamente inattesi e tantomeno comprensibili nelle loro conseguenze. Di fronte a tutto questo, il singolo utente da solo non può gestire e proteggersi dai rischi che si conoscono e ancor di più da quelli che si sviluppano in modo imprevedibile per l'intera comunità, basti pensare alle conseguenze sulle attività che può avere il cyber-crime o alle conseguenze sociali del cyber-bullismo. Sono le organizzazioni nazionali e sovranazionali che devono farsi carico di prevedere, proteggere ed informare le persone e le attività produttive da quello che il nuovo contesto sociale o tecnologico può determinare o sta già determinando. L'esigenza di regole e di controlli sulle attività private e professionali è dunque una necessità comune assolutamente doverosa da assolvere. Il nuovo Regolamento Europeo "GDPR" 2016/679 ha raccolto l'esigenza dell'intera comunità europea di tutelarsi in modo omogeneo e condiviso in merito a tutto ciò che riguarda il concetto alla base della privacy, e cioè il diritto alla tutela dei dati e delle informazioni della persona fisica per la salvaguardia della vita privata di ciascun individuo. Questo regolamento definisce ulteriormente, rispetto a quanto già presente, i diritti degli individui e le garanzie affinché questi diritti vengano tutelati da tutti coloro che possono avere a che fare con le loro informazioni. La tutela dei diritti nasce dal controllo che tutte le possibili entità coinvolte nella gestione delle informazioni personali rispettino le regole previste dal GDPR.

2. DEFINIZIONI

Articolo 4

Ai fini del presente regolamento s'intende per:

1) «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; (C26, C27, C30);
2) «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 l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;(C67)
4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)
5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)
6) «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; (C15)
7) «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; (C74)

8) «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;
9) «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; (C31)
10) «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;
11) «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; (C32, C33)
12) «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; (C85)
13) «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; (C34)
14) «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; (C51)
15) «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; (C35)
16) «stabilimento principale»: (C36, C37)
    a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (C80)

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: (C124)
   a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
   b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
   c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:
   a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro;

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. FAQ

Cosa è il Regolamento 2016/679?

Regolamento Europeo 2016/679 è il testo per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tra le misure privacy da adottare nel rispetto del Regolamento Europeo 679, c'è quella di redigere e conservare opportune documentazioni quali i Registri delle attività di trattamento secondo l'art. 30 (nel caso di imprese o organizzazioni con non meno di 250 dipendenti), in cui vengano riportare tutte le attività di trattamento dei dati svolte sotto la responsabilità del "titolare" al trattamento o del responsabile.
Viene richiesto anche di cooperare con l'autorità di controllo notificando qualsiasi violazione dei dati personali alla stessa e al diretto interessato entro 72 ore dal momento in cui se ne è venuti a conoscenza, all'autorità di controllo competente, e senza ingiustificato ritardo secondo l'art. 33.

Chi deve applicare il Regolamento 2016/679?

Il Regolamento Europeo è entrato in vigore il 25 maggio 2016 e si applicherà in tutti gli Stati Membri a partire dal 25 maggio 2018, termine entro il quale le aziende dovranno adeguarsi alla nuova legge sulla privacy. Con applicazione in tutti gli Stati Membri (a partire dal 25 maggio 2018) del regolamento Privacy 679, i Titolari e Responsabili del trattamento dovranno seguire il "principio della accountability" (art. 5 co. 2) che comporterà l'onere di dimostrare l'adozione, senza convenzionalismi, di tutte le misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Regolamento (art. 24-25 e l'intero CAPO IV).

Quali sono i dati personali?

I dati personali sono qualsiasi informazione relativa a una persona identificata o identificabile. Non c'è distinzione tra il ruolo pubblico, privato o lavorativo di una persona. I dati personali includono:

1. Nome
2. Indirizzo e-mail
3. Post sui social media
4. Informazioni fisiche, fisiologiche o genetiche
5. Informazioni mediche
6. Posizione
7. Dettagli bancari
8. Indirizzo IP
9. Cookie
10. Identità culturale

Quali sono i dati personali particolari?

I dati personali particolari sono:

1) Sensibili:
   a) adesioni a partiti o organizzazioni a carattere politico;
   b) adesione a sindacati o organizzazioni a carattere sindacale;
   c) convinzioni filosofiche;
   d) convinzioni religiose;
   e) immagini;
   f) opinioni politiche;
   g) origini etniche;
   h) origini razziali;
   i) vita sessuale;
2) giudiziari:
   a) informazioni di carattere giudiziario;
3) relativi alla salute:
   a) idoneità al lavoro;
   b) stato di salute;
   c) anamnesi familiare;
   d) patologie attuali e/o pregresse personali o relative a familiari;
   e) terapie in corso
4) biometrici;
5) genetici.

Quando sarà operativo il Regolamento?

I regolamenti UE sono immediatamente esecutivi e non richiedendo la necessità di recepimento da parte degli Stati Membri e garantiscono una maggiore armonizzazione a livello dell'intera UE.

Quali diritti devono essere garantiti dalle aziende ai sensi del Gdpr?

Il GDPR permette ai residenti nell'Unione Europea di controllare i dati attraverso una serie di "diritti degli interessati". Tra questi il diritto di:

1. Accedere a informazioni pronte e semplificate sulle modalità di utilizzo dei dati personali
2. Accedere ai dati personali
3. Far cancellare o correggere dati personali
4. Far correggere dati personali e cancellarli in determinate circostanze ("diritto di oblio")
5. Limitare o contestare l'elaborazione dei dati personali
6. Ricevere una copia dei dati personali
7. Rifiutarsi di elaborare dati per usi specifici, come ad esempio marketing o profiling

In che modo il Gdpr influenzerà la mia azienda?

Il GDPR include numerosi requisiti su raccolta, archiviazione e uso delle informazioni personali. Questo non include solo le modalità in cui identifichi e proteggi i dati personali nei tuoi sistemi, ma anche le modalità in cui rispetti i nuovi requisiti di trasparenza, rilevi e segnali le violazioni dei dati personali e sensibilizzi alla privacy il personale e i dipendenti.

Vista la moltitudine di elementi coinvolti, non dovresti aspettare che il regolamento abbia effetto per prepararti. Devi iniziare a rivedere subito le procedure di gestione dei dati e della privacy. La mancata conformità al GDPR potrebbe costare cara: le aziende che non soddisfano i requisiti e gli obblighi previsti rischiano gravi sanzioni e danni alla reputazione.

A quanto possono ammontare le sanzioni?

Le aziende sono passibili di sanzioni fino a 20 milioni di euro o fino al 4% del profitto annuo globale, a seconda di quale sia il valore maggiore, per la mancata applicazione di determinati requisiti del GDPR. Ulteriori rimedi individuali possono aumentare il rischio in caso di mancata adesione ai requisiti del GDPR.

Misure di sicurezza

Le misure di sicurezza previste sono:

1) Pseudonimizzazione;
2) Cifratura;

3) Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità la resilienza dei sistemi e dei servizi di trattamento;
4) Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
5) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Quanto segue rappresenta le specificità di Kangourou Italia nell'ambito del suesposto contesto

4. ATTIVITÀ DELL'ASSOCIAZIONE E DATI DEL TITOLARE

Titolare dei dati è ASSOCIAZIONE CULTURALE KANGOUROU ITALIA che ha la Sede Legale in Via Giacomo Medici 2, 20900 Monza (MB), Tel. (+39) 347 040 2755 – E-mail matematica@kangourou.it, pec kangourou.italia@pec.it, C.F. 94634130150 e P. IVA 09638180969, che ha per oggetto la diffusione della cultura matematica di base tra i giovani. Lo strumento operativo che, insieme ad altre associazioni facenti parte dell'Associazione Internazionale "Kangourou senza Frontiere", ha ideato per raggiungere tale scopo è la gestione e l'organizzazione di un gioco-concorso nazionale a cadenza annuale sulla matematica e la produzione degli strumenti editoriali collegati ad esso come i testi della gara, la pubblicazione di libri/articoli, manifesti, CD, giochi in varie forme.
Il legale rappresentante è Angelo Lissoni, C.F. LSSNGL49D29F704W.

5. ORGANIGRAMMA

Le persone che all'interno dell'ASSOCIAZIONE CULTURALE KANGOUROU ITALIA gestiscono i dati che rientrano nell'ambito del GDPR 679/2016 sono rappresentati nell' Allegato 2 che offre dettagli in merito alle persone a vario titolo coinvolte nell'Associazione.

6. ASSET

Poiché gli asset sono quei beni fisici ed informatici che supportano il business della Digital Transformation, occorre gestirli in modo da garantire la protezione dei dati.
Gli asset dell'ASSOCIAZIONE CULTURALE KANGOUROU ITALIA sono stati identificati nell'Allegato 3.
Per ogni asset è in essere un modus operandi per migliorarne la sicurezza.

7. TRATTAMENTI

I dati trattati riguardano:

1. Gestione concorso;
2. Gestione editoria;
3. Area Legale;
4. Area Consulenza per la Sicurezza Sui Luoghi di Lavoro;
5. Formazione;
6. Adempimenti civilistico-contabili;
7. Area Privacy.

7.1 GESTIONE CONCORSO

Titolare	Angelo Lissoni
Responsabile esterno	Cimidas incaricato attraverso il modulo Priv. 14
Tipologia di dati	Nominativo, telefono e indirizzo mail per i Docenti; Nominativo, Codice Fiscale e documenti identità per Studenti o per chi esercita la patria potestà.
Finalità	Gestione dei partecipanti al concorso, Gestione del contenzioso, Attività promozionali.
Causa	Il trattamento è necessario all'esecuzione di un contratto di cui gli utenti sono parte o all'esecuzione di misure precontrattuali adottate su richiesta degli stessi utenti.
Interessati	Utenti
Durata	I dati verranno conservati per il periodo strettamente necessario a garantire la corretta erogazione dei servizi acquistati – fatta salva la necessità di conservazione per un periodo più lungo in osservanza della normativa, anche contabile, applicabile.
Raccolta	Il consenso viene rilasciato al momento dell'acquisizione dei dati personali (che avviene al momento dell'iscrizione al gioco-concorso di cui al punto 4) attraverso l'Allegato 1A (Docenti) e l'Allegato 1B (Studenti), tramite procedure informatiche.
Asset	Vedi allegato Asset
Destinatari	Utenti i cui dati vengono utilizzati per la gestione del concorso e per la pubblicazione sul sito dell'Associazione nel caso in cui risultino ammessi alle fasi successive del concorso o risultino vincitori.
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Incaricati	Soci e/o collaboratori esterni (da 1 a 8 dell'organigramma in Allegato 2).

Minori	Possibile trattamento minori ma solo con il consenso dei genitori o di chi ne ha la patria potestà
Paesi esteri	Non vi è un trasferimento verso paesi esteri o verso organizzazioni internazionali.
Automatizzazione o Profilazione	Nel trattamento non sono presenti processi automatizzati di raccolta dati o metodi di profilazione

7.2 GESTIONE SPEDIZIONI

Titolare	Angelo Lissoni
Responsabile esterno	3tLogistica incaricato attraverso il modulo Priv. 14
Tipologia di dati	Nominativo del responsabile/docente, nominativo ed indirizzo della scuola
Finalità	Gestione della clientela, Adempimenti civilistico contabili, Gestione delle criticità
Causa	Il trattamento è necessario all'esecuzione del contratto di cui gli utenti sono parte o all'esecuzione di misure precontrattuali adottate su richiesta degli utenti stessi.
Interessati	Utenti
Durata	I dati verranno conservati per il periodo strettamente necessario a garantire la corretta erogazione dei servizi acquistati, fatta salva la necessità di conservazione per un periodo più lungo in osservanza della normativa, anche contabile, applicabile.
Raccolta	Il consenso viene rilasciato al momento dell'acquisizione dei dati personali attraverso il modulo Priv. 11. tramite procedure informatiche.
Asset	Vedi allegato Asset
Destinatari	Utenti i cui dati vengono utilizzati per la consegna del materiale inerente il gioco-concorso annuale di cui al punto 4.
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Incaricati	Soci e/o collaboratori esterni (da 1 a 8 dell'organigramma in Allegato 2).
Minori	Nessun trattamento per minori
Paesi esteri	Non vi è un trasferimento verso paesi esteri o verso organizzazioni internazionali.
Automatizzazione o Profilazione	Nel trattamento non sono presenti processi automatizzati di raccolta dati o metodi di profilazione

7.3 AREA LEGALE

Titolare	Angelo Lissoni
Responsabile esterno	Professionista di volta in volta incaricato attraverso il modulo M Priv. 14
Tipologia di dati	Dati personali particolari "giudiziari", dati personali relativi ad attività economico finanziarie assicurative
Casistica per il trattamento dati	Necessari per esercitare o difendere un diritto in sede giudiziaria o dirimere contenziosi
Finalità	Il trattamento è necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento
Interessati	Interessato al presente trattamento è ogni stakeholders dell'Associazione.
Durata	I dati verranno trattati per tutta la durata del rapporto contrattuale instaurato e anche successivamente, per l'espletamento di tutti gli adempimenti di legge. I dati verranno conservati per il periodo strettamente necessario a garantire la corretta erogazione dei servizi acquistati – salva la necessità di conservazione per un periodo più lungo in osservanza della normativa, anche contabile, applicabile.
Raccolta	La raccolta dei dati non avviene tramite informativa in quanto lo studio legale tratta dati, forniti dall'associazione stessa, nel rispetto del segreto professionale e perché l'interessato dispone già delle informazioni in quanto lavoratore dipendente o cliente/fornitore.
Asset	I dati relativi alle varie pratiche sono tenuti nell'archivio presso l'ufficio della Direzione, nei Pc della Direzione.
Destinatari	Destinatari esterni possono essere altri uffici giudiziari, l'autorità giudiziaria o, in rari casi, altri consulenti che svolgono una funzione tecnica
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Minori	Il trattamento potrebbe riguardare indirettamente minori
Paesi esteri	Non vi è un trasferimento verso paesi esteri o verso organizzazioni internazionali.
Automatizzazione o Profilazione	Nel trattamento non sono presenti processi automatizzati ~~o~~ metodi di profilazione.

7.4 SICUREZZA NEGLI EVENTI

Titolare	Angelo Lissoni
Responsabile esterno	Professionista di volta in volta individuato nei luoghi degli eventi, condividendo documento di supervisione con dichiarazione di regolarità.
Tipologia di dati	Dati personali dei lavoratori (dati di contatto, identificativi, dati sul comportamento, profili di fornitori etc.)

Finalità	Il trattamento è necessario per adempiere agli obblighi legali previsti dal D.Lgs. 81/08 al quale è soggetto chi ospita l'evento.
Interessati	Interessato al presente trattamento è ogni stakeholders dell'Associazione.
Durata	I dati verranno trattati per l'espletamento di tutti gli adempimenti di legge.
Raccolta	La raccolta dei dati non avviene tramite informativa in quanto il consulente tratta dati forniti dall'ente che ospita l'evento e/o perché l'interessato dispone già delle informazioni.
Asset	I dati relativi alle varie pratiche sono tenuti nell'archivio presso l'ufficio dell'Associazione e/o dall'ente che ospita l'evento.
Destinatari	I dati possono essere comunicati ad altri consulenti, agli enti di sorveglianza che esercitano controllo sull'evento (es. Asl, Polizia Postale e Guardia di Finanza).
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Minori	Il trattamento potrebbe riguardare minori
Paesi esteri	Non vi è un trasferimento verso paesi esteri o verso organizzazioni internazionali.
Automatizzazione o Profilazione	Nel trattamento non sono presenti processi automatizzati o metodi di profilazione.

7.5 AREA FORMAZIONE

Titolare	Angelo Lissoni
Responsabile esterno	Eventuale Professionista incaricato attraverso il modulo Priv. 14
Tipologia di dati	Dati personali dei partecipanti all'intervento formativo
Finalità	Il trattamento è necessario per adempiere agli obblighi contrattuali.
Interessati	Interessati al presente trattamento sono i partecipanti all'intervento formativo.
Durata	I dati verranno trattati per tutta la durata del rapporto contrattuale instaurato e anche successivamente, per l'espletamento di tutti gli adempimenti di legge e per l'invio d'informative relative alla promozione di nuove attività formative.
Raccolta	La raccolta dei dati non avviene tramite informativa in quanto il consulente tratta dati forniti dalla Direzione dell'Associazione o perché l'interessato dispone già delle informazioni in quanto collaboratore.
Assets	I dati relativi alle varie pratiche sono tenuti nell'archivio presso l'ufficio dell'Associazione.
Destinatari	I dati possono essere comunicati ad altri consulenti, agli enti di sorveglianza e controllo (es. Asl, Polizia Postale e Guardia di Finanza).
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

	Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Minori	Il trattamento non riguarda minori
Paesi esteri	Non vi è un trasferimento verso paesi esteri o verso organizzazioni internazionali.
Automatizzazione o Profilazione	Nel trattamento non sono presenti processi automatizzati o metodi di profilazione.

7.6 ADEMPIMENTI CIVILISTICO-FISCALI

Titolare	Angelo Lissoni
Responsabile esterno	Studio Romeo attraverso il modulo Priv.14
Tipologia di dati	Dati comuni identificativi dei collaboratori, dei fornitori e degli stakeholders dell'Associazione, dati economici, patrimoniali, finanziari (anche coordinate bancarie), assicurativi, commerciali (dati di comunicazione e contatto), personali dei lavoratori (dati di contatto, identificativi, etc.), etc.
Finalità	Trattamento relativo all'attività di gestione degli adempimenti contabili, giuslavoristici, amministrativi, fiscali.
Causa	Necessario per assolvere gli obblighi civilistico fiscali ed esercitare i diritti specifici del titolare del trattamento.
Interessati	Interessati al presente trattamento sono, i consulenti liberi professionisti o meno, i lavoratori autonomi, i fornitori ed ogni altro stakeholder dell'Associazione
Durata	I Dati personali verranno trattati per tutta la durata dell'incarico ed anche successivamente per far valere o tutelare i propri diritti ovvero per finalità amministrative e/o per dare esecuzione ad obblighi derivanti dal quadro regolamentare e normativo pro tempore applicabile e nel rispetto degli specifici obblighi di legge sulla conservazione dei dati
Raccolta	La raccolta dei dati non avviene tramite informativa in quanto l'interessato dispone già delle informazioni poiché collabora con l'azienda già da tempo ed ha potuto vedere la Privacy Policy e discuterla con l'Associazione.
Asset	Tutti gli asset aziendali
Incaricati	Roberta Lissoni
Destinatari	Agenzia delle entrate, altre amministrazioni pubbliche, autorità giudiziaria, banche ed altri istituti di credito o finanziari o assicurativi, Camere di Commercio, consulenti e liberi professionisti, Inail, Inps, Enti di certificazione e laboratori, eventuali altre società o imprese.
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Minori	Il trattamento non riguarda minori

Paesi esteri	Non vi è un trasferimento verso paesi esteri o verso organizzazioni internazionali.
Automatizzazione o Profilazione	Nel trattamento non sono presenti processi automatizzati o metodi di profilazione.

7.7 AREA PRIVACY

Titolare	Angelo Lissoni
Responsabile esterno	Punto e Linea Consulting Srl rappresentata dal Dr. Alessandro Ancilotti attraverso il modulo Priv. 14
Tipologia di dati	Dati personali relativi allo svolgimento dei processi aziendali, dati personali dei collaboratori (dati di contatto, identificativi).
Finalità	Il trattamento è necessario per adempiere all'attività di consulenza tali da comprendere la gestione dei dati personali
Interessati	Interessato al presente trattamento sono ogni stakeholder dell'Associazione
Durata	I dati verranno trattati per tutta la durata del rapporto contrattuale instaurato e anche successivamente, per l'espletamento di tutti gli adempimenti di legge.
Raccolta	La raccolta dei dati avviene tramite informativa sebbene il consulente tratti dati, forniti dall'Associazione stessa, nel rispetto del segreto professionale e perché l'interessato dispone già delle informazioni.
Asset	I dati relativi alle varie pratiche sono tenuti nell'archivio presso l'ufficio della Direzione, nei Pc della Direzione, nel sistema informatico del consulente e nei Pc della contabilità.
Destinatari	I dati possono essere comunicati alle autorità giudiziarie che li richiedessero per l'espletamento degli obblighi normativi.
Misure di Sicurezza	La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Test, verifiche e valutazioni periodiche dell'efficacia delle misure tecniche e organizzative finalizzate a garantire la sicurezza del trattamento.
Minori	Il trattamento può riguardare indirettamente minori durante le attività di Audit.
Paesi esteri	Nel trattamento non è presente un trasferimento verso paesi esteri o verso organizzazioni internazionali.
~~Automatizzazione e~~ Profilazione	Nel trattamento non sono presenti processi automatizzati o metodi di profilazione.

8. VALUTAZIONE D'IMPATTO (DPIA)

Uno dei cardini fondamentali del nuovo GDPR è la valutazione del livello di sicurezza. Con l'introduzione di tale elemento, si è tenuti a valutare i rischi derivati dal trattamento in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale dei dati trasmessi, conservati o comunque trattati.

Vedi Allegato 4 "Analisi Rischi".

9. AUDIT

L'Audit Privacy è una valutazione del livello di adesione alla normativa vigente; è un vero e proprio check up che deve essere effettuato da un esperto indipendente con un buon grado di conoscenza in ambito di protezione dei dati sia a livello giuridico che informatico.

Ci sono due tipi di audit privacy:

1) audit di adeguatezza
2) audit di conformità

L'audit di adeguatezza ha l'obiettivo di:

1. Determinare se le politiche privacy sono adeguate per rispondere e rispettare tutti i requisiti legali;
2. Assicurare che le politiche privacy corrette siano applicate a tutti i trattamenti dati svolti dall'organizzazione.

Questo tipo di audit coinvolge la revisione non solo delle politiche, procedure e istruzioni operative, che interessano la gestione dei dati personali, ma anche delle politiche relative alle terze parti come i fornitori, richiedendo di comprendere e mappare il flusso dei dati dell'Associazione.

Un audit di adeguatezza può rilevare gravi lacune nelle politiche di privacy dei dati di un'organizzazione, partendo dai tipi di trattamento dei dati personali e dalle modalità in cui sono archiviati, trasferiti e trattati.

In questo caso è consigliabile prima di proseguire, effettuare una verifica e correzione delle politiche e procedure privacy per poi realizzare un audit di conformità.

L'audit di conformità richiede che l'indagine dei dati personali sia gestita trasversalmente tra i vari soggetti coinvolti e con i fornitori.

Un efficace audit di conformità deve anche esaminare come l'organizzazione realizza la formazione sulla privacy, e come si pensa di gestire eventuali reclami circa la violazione della privacy.

Gli strumenti per realizzare gli audit privacy sono:

1) questionari/ interviste di follow-up con l'obiettivo di mappare i processi e flussi dei dati.
2) Una tabella matrice che consenta la tabulazione e l'organizzazione dei risultati dell'audit

10. DATA BREACH

Una delle novità più rilevanti introdotte dal nuovo Regolamento UE sulla Protezione dei dati (GDPR) è l'obbligo, per amministrazioni pubbliche e aziende, di comunicare all'autorità di controllo competente i casi di Data Breach (l´obbligo di comunicare eventuali violazioni di dati personali) quindi, tutte le violazioni della sicurezza IT in grado di comportare la perdita, distruzione o diffusione indebita dei dati personali trattati. Il mancato adempimento comporta l'imposizione di sanzioni previste dal GDPR.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato. Il termine per adempiere alla notifica è brevissimo, settantadue ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

Rev. 0 del 9/12/2020

Monza, 10 dicembre 2020



Angelo Lissoni

ALLEGATI

All. 1A (accettazione privacy docenti) e 1B (accettazione privacy studenti)

All. 2 Organigramma

All. 3 Asset

All. 4 PIA - Valutazione Rischi Impatto Trattamento dati