Polizza multirischi dell'Agente di assicurazione: Responsabilità Civile Professionale e Garanzie complementari

ALLEGATO N. 1 – CYBER RISK

Mod POL AG GR Cyber Risk

www.cgpa-europe.it

CGPA Europe S.A. Rappresentanza Generale per l'Italia
Largo Castello, 28 - 44121 Ferrara
C. F. e Part. IVA 12140021002 – Codice IVASS D912R

Società di assicurazioni registrata in Lussemburgo
con n. B170142 – 41, boulevard Royal - L-2449 Lussemburgo

Sommario

ALLEGATO N. 1

Condizioni Speciali

GARANZIE AGGIUNTIVE

del "CYBER RISK"

1 - Le garanzie aggiuntive regolamentate nel presente allegato sono complementari e sono valide soltanto se il Contraente ne ha chiesto l'attivazione esercitando, per conto dell'Assicurato, l'opzione di beneficiarne verso pagamento del relativo premio. Se le garanzie sono attivate, le rispettive somme assicurate e massimali figurano nella Scheda di Polizza.

2 - Salvo quanto stabilito nel presente allegato, si applicano tutte le Definizioni e Condizioni Generali della polizza.

CR.1 Definizioni aggiuntive

Per l'interpretazione delle presenti Condizioni Speciali, le parti fanno riferimento alle definizioni esposte qui di seguito in ordine alfabetico. Per gli altri termini usati nelle condizioni del presente allegato e nelle Condizioni Generali di polizza, le parti fanno riferimento alle definizioni che figurano nella Sezione Prima della polizza. Nel testo che segue le definizioni aggiuntive figurano in carattere corsivo e con iniziali maiuscole.

(a) ATTIVITA' MULTIMEDIALI - Qualsiasi testo, immagine, video o suono, divulgati dall'Assicurato tramite una propria pagina web o con l'utilizzo di social media o di email.

(b) COSTI DI DIFESA - Gli onorari e altri compensi sostenuti dall'Assicurato per la difesa dei suoi interessi a seguito di una richiesta di risarcimento o di un *Fatto Dannoso*. Tali costi comprendono espressamente gli onorari degli avvocati, dei periti e degli esperti, le spese per procedure e quelle giudiziali.

In nessun caso rientrano nei *Costi di Difesa* gli stipendi o retribuzioni dei dipendenti dell'Assicurato né le cauzioni che l'Assicurato sia eventualmente tenuto a versare in caso di processo, inchiesta, istruttoria o indagine.

(c) DANNEGGIAMENTO DI DATI - Il furto, la perdita o la divulgazione non autorizzata di *Dati Personali* in possesso o in custodia dell'Assicurato o di una persona del cui operato l'Assicurato sia legalmente tenuto a rispondere.

(d) DANNEGGIAMENTO DEI SISTEMI - Le azioni sotto enumerate, qualora configurino una *Violazione della Sicurezza* :

1. alterazione, corruzione, distruzione, soppressione o *Danneggiamento di Dati Protetti*
2. *Programma di Malware* che dal *Sistema Informatico* venga trasmesso su un *Sistema Informatico Esterno*
3. il coinvolgimento del *Sistema Informatico* in un *Diniego di Servizi* diretto contro un *Sistema Informatico Esterno*.

(e) DATI PROTETTI Le informazioni digitali in possesso dell'Assicurato per lo svolgimento dell'Attività Esercitata, qualunque ne sia la forma o il metodo di utilizzazione o visualizzazione (testo, immagini, video, o altro), immagazzinate nei *Sistemi Informatici* che siano oggetto di una periodica procedura di salvataggio informatico, ossia:

- DATI PERSONALI - Le informazioni che identificano o possono identificare una persona fisica, a norma di quanto disposto dalla normativa in vigore, ivi compresi i dati soggetti a trattamento speciale quali, tra l'altro, stato di salute, convinzioni religiose o filosofiche, appartenenza sindacale, vita sessuale. Non costituiscono "Dati Personali" le informazioni messe liberamente a disposizione dalla Pubblica Amministrazione;
- DATI AZIENDALI – Le informazioni che riguardano una persona giuridica e ne rivelano informazioni riservate, quali: segreto industriale, progetti, disegni, formule, metodi, prassi, procedimenti, informazioni di carattere contabile, finanziario o di marketing, segreto professionale.

Rientrano in questa definizione i programmi informatici, i software e le applicazioni che acquisiscono, trattano e archiviano i suddetti dati ed informazioni.

(f) DINIEGO DI SERVIZI - Attacco informatico volto deliberatamente ad esaurire le risorse di un qualunque sistema informatico, fino a renderlo incapace di erogare servizi ai client richiedenti ("DoS: Denial of Service" o "DDoS: Distributed Denial of Service").

(g) ERRORE UMANO - Negligenza o imperizia commessa da un dipendente o preposto dell'Assicurato, nell'utilizzo dei *Sistemi Informatici* nell'ambito dell'Attività Esercitata.

(h) FATTO DANNOSO - Il fatto che è causa di un danno e/o di una responsabilità nei casi previsti dalle garanzie prestate nel presente allegato. Ai fini di queste garanzie, l'insieme di *Fatti Dannosi* originati da una stessa causa è ritenuto un unico *Fatto Dannoso*.

(i) FORNITORE DI SERVIZI - Il fornitore esterno di applicazioni informatiche residenti presso l'Assicurato, oppure il fornitore che gestisce, predispone, detiene o conserva i dati dell'Assicurato in virtù di un contratto con lui stipulato.

(j) LIMITE DI INDENNIZZO GLOBALE - L'ammontare esposto nella Scheda di Polizza, che rappresenta l'esborso cumulativo massimo a carico della Società Assicuratrice per tutti i *Sinistri* di pertinenza di un *Periodo di Assicurazione* e per l'insieme di tutte le garanzie disciplinate da questo allegato.

Il *Limite di Indennizzo Globale* di un *Periodo di Assicurazione* non si cumula in nessun caso con quello di un periodo precedente o successivo, né in conseguenza di proroghe, rinnovi o sostituzioni del contratto o di questo allegato, né per il cumularsi dei premi pagati o da pagare.

(k) MINACCIA DI ESTORSIONE - *Violazione della Sicurezza* a mezzo minaccia di:

1. alterare, distruggere, danneggiare, cancellare o infettare qualunque *Dato Protetto*;
2. impedire l'accesso ai *Sistemi Informatici* o a un *Dato Protetto*, anche per mezzo di un *Diniego di Servizi* o della criptazione di un *Dato Protetto* rendendolo inaccessibile;
3. commettere il furto o l'uso illecito di un *Dato Protetto*, attraverso un accesso esterno;
4. introdurre un programma di malware su un *Sistema informatico*;
5. provocare l'interruzione o la sospensione di un *Sistema informatico*.

(l) NORME SULLA NOTIFICA DELLA VIOLAZIONE - Le norme di legge o di regolamento, qualunque sia lo Stato o l'autorità amministrativa che le abbia emanate, che impongano di informare le persone i cui *Dati Personali* siano colpiti da una di *Violazione della Sicurezza*.

(m) PENALITÀ PCI-DSS - Le sanzioni e penalità dovute dall'Assicurato in virtù di un contratto PCI-DSS (Payment Card Industry – Data Security Standard), ossia un contratto stipulato con un *Fornitore di Servizi* di pagamento o di sistemi di pagamento, allo scopo di permettere all'Assicurato di ricevere e accettare pagamenti a mezzo di carta di credito, carta di debito o documento analogo. Non rientrano in questa definizione: i costi sostenuti o da sostenere, i "charge backs", gli "interchange fees", i "discount fees".

(n) PERIODO DI ASSICURAZIONE - Il periodo che intercorre dalla data in cui questo allegato entra in vigore e la data di scadenza indicata nella Scheda della polizza della quale questo allegato forma parte.

(o) PROGRAMMA DI MALWARE - Qualunque programma o software destinato intenzionalmente a inserirsi nella memoria informatica o su un disco informatico per diffondersi da un computer a un altro, quali ad esempio: cavallo di troia, virus, baco, codice o script.

(p) PROTOCOLLO PER LA PROTEZIONE DEI DATI ("Privacy Policy") - Le dichiarazioni scritte e pubblicate dall'Assicurato o chi per lui in merito alla sua politica riguardante la raccolta, utilizzazione, divulgazione, condivisione, correzione o modificazione di *Dati Personali*, nonché l'accesso a tali informazioni. Il protocollo è inteso a:

1. proibire o limitare la divulgazione, la condivisione o la vendita di *Dati Personali* da parte dell'Assicurato
2. dichiarare che l'Assicurato è tenuto a permettere l'accesso ai *Dati Personali* agli interessati che ne facciano richiesta o a correggere tali dati se risultanti incompleti o inesatti
3. stabilire procedure e condizioni per prevenire la perdita di *Dati Personali*.

(q) SICUREZZA INFORMATICA - I software, i computer e i dispositivi collegati, nonché le procedure predisposte per iscritto dall'Assicurato ai fini di prevenire un *Danneggiamento dei Sistemi*. La *Sicurezza Informatica* comprende i software antivirus e di rilevamento delle intrusioni, le barriere di sicurezza e i sistemi elettronici che attuano il controllo dell'accesso ai *Sistemi Informatici* utilizzando una password o l'identificazione biometrica o altri metodi equivalenti per individuare gli utilizzatori autorizzati.

(r) SINISTRO

I. Il verificarsi, nel corso del *Periodo di Assicurazione*, di un *Fatto Dannoso* rientrante tra quelli previsti dalle garanzie A, D, E, F, G, H, I di questo allegato.

II. La richiesta di risarcimento avanzata da *Terzi* contro l'Assicurato per la prima volta durante il *Periodo di Assicurazione*, per perdite patrimoniali cagionate da un *Fatto Dannoso* rientrante tra quelli previsti dalle garanzie B e C di questo allegato. Come stabilito alla definizione 11 figurante nella Sezione Prima della polizza, le richieste di risarcimento derivanti da uno stesso *Fatto Dannoso*, anche se avanzate da persone diverse, danno luogo a un unico *Sinistro;* in questo caso, la data della prima richiesta di risarcimento sarà considerata come data di tutte quelle successive.

(s) SISTEMA INFORMATICO - I computer e i rispettivi dispositivi periferici e di immagazzinamento dei dati, gli strumenti collegati e le installazioni di salvataggio, il tutto gestito dall'Assicurato che ne sia proprietario o locatario oppure gestito da un *Fornitore di Servizi*.

(t) SISTEMA INFORMATICO ESTERNO - *Sistema informatico* che non appartiene, non è gestito né controllato dall'Assicurato o da un suo *Fornitore di Servizi*, con l'avvertenza che non è considerato esterno il sistema informatico di *Terzi* sui quali l'Assicurato realizza dei servizi.

(u) TEAM DI PRONTO INTERVENTO - Il team nominato dalla Società assicuratrice il cui compito è il coordinamento e la gestione dei *Sinistri* rientranti nella garanzia A (Assistenza e gestione degli eventi).

(v) TERZO/TERZI - Ogni soggetto così definito alla definizione 6 figurante nella Sezione Prima della polizza, ma compresi – purché non siano autori o co-autori del *Fatto Dannoso* – i dipendenti di cui alla definizione 7 e le persone indicate alla voce 2.c della definizione 2.

(w) VIOLAZIONE DELLA SICUREZZA

1. L'accesso o l'utilizzo abusivi dei *Sistemi Informatici*, anche a seguito del furto di una password
2. il *Diniego di Servizi* che colpisca i *Sistemi Informatici* o i *Sistemi Informatici Esterni*
3. gli effetti di un *Programma di Malware* che vada a infettare i *Sistemi Informatici* o che da questi venga trasmesso su altri programmi.

La violazione può essere diretta verso singoli Assicurati o di portata più generale.

Una serie di *Violazioni della Sicurezza* derivanti da una stessa causa e risultanti specificamente da una stessa inosservanza della *Sicurezza Informatica* sarà considerata un'unica *Violazione della Sicurezza* verificatasi al momento della prima di tali violazioni.

CR.2 Oggetto delle garanzie "Cyber Risk"

Fino a concorrenza delle somme assicurate e dei massimali indicati nella Scheda di Polizza, l'assicurazione è prestata verso pagamento del premio convenuto, alle Condizioni Generali di polizza e alle Condizioni Speciali esposte nei paragrafi che seguono.

A - Assistenza e gestione degli eventi

(forma «losses occurring»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato dei costi degli interventi messi in atto a seguito di *Danneggiamento di Dati* o di *Danneggiamento dei Sistemi*, reali o presunti, che si verifichino durante il *Periodo di Assicurazione*. Tali interventi concernono:

A.1 *Sicurezza Informatica*

1. L'accertamento compiuto da un esperto in *Sicurezza Informatica* sull'esistenza, la causa e l'ampiezza del *Danneggiamento di Dati* e/o del *Danneggiamento dei Sistemi*, nonchè i costi da sostenere allo scopo di limitare gli effetti del *Danneggiamento dei Sistemi* e di porvi rimedio.
2. L'analisi compiuta da un esperto in *Sicurezza Informatica* sulla capacità dell'Assicurato di evitare un analogo incidente in futuro, purché tale analisi sia richiesta a seguito di un obbligo contrattuale assunto dall'Assicurato.
3. L'analisi compiuta da un esperto abilitato dall'Ente responsabile degli standard di protezione PCI-DSS, incaricato dall'Assicurato di indagare sull'esistenza e l'ampiezza di una violazione, reale o presunta, di dati delle carte di pagamento digitale, a condizione che la predetta analisi sia la conseguenza di un obbligo contrattuale scritto a carico dell'Assicurato. Le indagini di questo esperto si svolgono sotto la supervisione dell'esperto in *Sicurezza Informatica* di cui al precedente punto 1), i cui onorari sono a carico della Società Assicuratrice.

A.2 Difesa legale

1. La consultazione di un avvocato incaricato di fornire assistenza legale all'Assicurato al fine di limitare gli effetti del *Danneggiamento di Dati* o *Danneggiamento dei Sistemi*.
2. La consultazione di un avvocato o di un esperto legale incaricato di consigliare l'Assicurato sulle misure da prendere in caso di violazione, reale o presunta, dei dati delle carte di pagamento digitale, a condizione che tali misure siano contrattualmente previste a carico dell'Assicurato. Sono esclusi dalla presente

garanzia i *Costi di Difesa* in procedure relative a *Penalità PCI-DSS* e gli onorari per consultazioni sull'applicabilità di tali penalità.

A.3 Notifiche prescritte

Le comunicazioni di notifica che in base alle *Norme sulla Notifica della Violazione* bisogna dare alle singole vittime di danno alla loro reputazione, ai loro beni o interessi, a causa della violazione dei *Dati Personali* che li riguardano. Le notifiche indicheranno il numero da chiamare per l'assistenza telefonica.

A.4 Assistenza telefonica

Servizio di assistenza telefonica messo a disposizione delle persone a cui è stata inviata la notifica di cui al punto A.3, alle quali verranno fornite le informazioni che l'Assicurato è tenuto a comunicare in forza della normativa vigente in materia. Il servizio è operativo nei giorni e nelle ore d'ufficio e sarà disponibile per un periodo di novanta (90) giorni di calendario (o per un periodo maggiore se richiesto dalla legge) da conteggiarsi dalla data in cui la notifica è stata inviata.

A.5 Vigilanza internet

La vigilanza e il monitoraggio internet sulla comparsa di *Dati Personali* riguardanti ognuna delle persone a cui è stata inviata la notifica di cui al punto A.3.

La vigilanza comprende il monitoraggio del credito, ossia l'intervento di un *Fornitore di Servizi* approvato dalla Società Assicuratrice, per il monitoraggio del profilo creditizio e per la protezione contro le frodi, allo scopo di rilevare eventuali usi impropri dei dati (ad es., domande di credito, aperture di conti, cambiamenti di indirizzo) a seguito di una *Violazione della Sicurezza.*

I costi della vigilanza in rete e del monitoraggio del credito sono a carico della Società Assicuratrice a condizione che siano sostenuti entro e non oltre i dodici (12) mesi successivi alla denuncia di un *Sinistro* o di un attacco, siano necessari per evitare *Sinistri* in futuro e siano preventivamente approvati dalla Società Assicuratrice.

B - Responsabilità civile

(forma «claims made»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato delle perdite patrimoniali e dei *Costi di Difesa* che egli sia tenuto a pagare per richieste di risarcimento avanzate da *Terzi* nei

suoi confronti durante il *Periodo di Assicurazione* (salva la copertura postuma stabilita all'articolo CR.4), ove tali richieste derivino da responsabilità dell'Assicurato per:

1. *Danneggiamento di Dati* o *Danneggiamento dei Sistemi*, compresa la violazione, reale o asserita, di una norma in vigore in materia di protezione dei *Dati Protetti;*
2. Mancata o tardiva comunicazione agli interessati, come prescritto dalle *Norme sulla Notifica della Violazione,* in caso di *Danneggiamento di Dati* o di *Danneggiamento dei Sistemi;*
3. Inosservanza del *Protocollo per la Protezione dei Dati*, a condizione che il protocollo sia in vigore al momento degli errori, delle azioni o delle omissioni che motivano la richiesta di risarcimento.

C - Responsabilità connessa ad *Attività Multimediali*

(forma «claims made»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato delle perdite patrimoniali e dei *Costi di Difesa* che egli sia tenuto a pagare per richieste di risarcimento avanzate nei suoi confronti durante il *Periodo di Assicurazione* (salva la copertura postuma stabilita all'articolo CR.4), ove tali richieste derivino da responsabilità dell'Assicurato per effetto di taluno dei seguenti fatti commessi nell'ambito dell'esecuzione di *Attività Multimediali*:

1. diffamazione, calunnia, denigrazione, ingiuria, danno alla reputazione, al buon nome o all'onorabilità di una persona fisica o giuridica;
2. violazione della vita privata o del diritto all'immagine;
3. appropriazione indebita di un nome o una denominazione, o imitazione dell'aspetto di cose, per fini commerciali;
4. plagio, azione piratesca o appropriazione indebita di idee in violazione di un contratto, anche tacito, sulla titolarità di tali idee;
5. inosservanza di diritti d'autore, di copyright, di marchi, disegni e modelli, del diritto dei produttori e dei proprietari di banche-dati, e più in generale del diritto al nome di un dominio, un marchio, un'insegna commerciale, un logo, un titolo, un metatag, uno slogan;
6. operazioni di "*deep linking*" o di "*framing*" di un contenuto in rete.

D - Danni all'immagine dell'Assicurato

(forma «losses occurring»)

In caso di pubblicazione o divulgazione, effettiva o imminente, a mezzo stampa o su mezzi audiovisivi, di un *Sinistro* coperto da taluna delle garanzie disciplinate in questo allegato, la Società Assicuratrice si obbliga a tenere indenne l'Assicurato dei costi da lui sostenuti allo scopo di ridurre i danni alla propria immagine e al suo prestigio professionale. Tali costi si riferiscono a:

- intervento di un consulente in pubbliche relazioni o in gestione delle criticità
- diffusione di annunci e messaggi al pubblico
- notificazione volontaria a singoli soggetti (compresi le spese annesse e connesse) nel corso dei novanta (90) giorni successivi alla prima rivelazione al pubblico di un danno all'immagine.

Resta inteso che tali costi dovranno essere previamente approvati dalla Società Assicuratrice, la quale non rifiuterà la sua approvazione senza validi motivi, e dovranno essere proporzionati alla gravità del danno oggettivamente subito o temuto.

E - Procedimenti amministrativi

(forma «claims made»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato dei *Costi di Difesa* in caso di procedure amministrative, ispezioni o inchieste in merito all'inosservanza, reale o asserita, degli obblighi di legge o di regolamento, promossa a carico dell'Assicurato dall'Autorità Garante della protezione dei dati personali, dalla Polizia postale o da qualunque altro ente nazionale, sovranazionale o estero competente in materia, a seguito di *Danneggiamento di Dati* o di *Danneggiamento dei Sistemi*, resi noti nel corso del *Periodo di Assicurazione,* anche se risalenti a epoca anteriore, con retroattività illimitata se non diversamente indicato nella Scheda di Polizza.

Questa garanzia non è operante rispetto a qualunque altra procedura d'inchiesta fondata su motivi diversi dal verificarsi di detti Danneggiamenti.

Le sanzioni eventualmente irrogate all'Assicurato sono escluse da questa garanzia.

F - Penalità PCI-DSS

(forma «claims made»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato delle *Penalità PCI-DSS* che egli sia tenuto a pagare nel corso del *Periodo di Assicurazione* (salva la copertura Postuma stabilita dall'art. CR.4), a condizione che le penalità vengano inflitte in ragione di una violazione reale o asserita delle norme per la sicurezza PCI-DSS e di effettivo o presunto *Danneggiamento di Dati* o *Danneggiamento dei Sistemi*, anche se risalenti a epoca anteriore, con retroattività illimitata se non diversamente indicato nella Scheda di Polizza.
I *Costi di Difesa* restano esclusi da questa garanzia.

G - Cyber Extortion

(forma «losses occurring»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato dei costi sotto elencati, da sostenere previo consenso scritto della Società Assicuratrice, qualora l'Assicurato si veda costretto a pagarli per porre fine a una *Minaccia di Estorsione* posta in essere per la prima volta nel corso del *Periodo di Assicurazione* :

1. qualunque pagamento in denaro o in forma specifica, effettuato sotto ricatto, da o per conto dell'Assicurato;
2. i compensi e onorari pagati dall'Assicurato o da chi per lui a un consulente.

La Società Assicuratrice tiene indenne l'Assicurato in caso di perdita, distruzione o sparizione del denaro o dei beni destinati al pagamento suddetto, durante il trasferimento effettuato da una o più persone incaricate dall'Assicurato o da chi per lui.

L'obbligazione della Società Assicuratrice è subordinata:

a. alla dimostrazione da parte dell'Assicurato che il pagamento è eseguito sotto ricatto;
b. all'impegno dell'Assicurato, d'intesa con la Società Assicuratrice, di dare avviso della *Minaccia di Estorsione* alla Polizia Postale o a qualunque altra autorità pubblica.

La *Minaccia di Estorsione* deve essere denunciata alla Società Assicuratrice entro i cinque (5) giorni dalla data in cui l'Assicurato l'ha ricevuta.

H - Ripristino dei dati

(forma «losses occurring»)

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato dei costi ragionevolmente sostenuti e necessari allo scopo di ripristinare o di riavere accesso ai dati alterati, infetti,

distrutti, cancellati o danneggiati per effetto di *Danneggiamento dei Sistemi* o di un *Errore Umano* che si siano manifestati per la prima volta all'Assicurato nel corso del *Periodo di Assicurazione*.

I - Perdite patrimoniali conseguenti a un *Sinistro*

(forma «losses occurring»)

I.1 - Perdita di reddito

La Società Assicuratrice si obbliga a tenere indenne l'Assicurato della perdita di reddito subita durante il periodo di interruzione purché sia la conseguenza diretta di un'interruzione o sospensione effettiva e inevitabile dei *Sistemi Informatici*, avvenuta per la prima volta nel corso del *Periodo di Assicurazione* e risultante direttamente da *Danneggiamento dei Sistemi* o da *Errore Umano*.

La perdita di reddito consiste nella riduzione del Margine Operativo Lordo (MOL) – dato dalla differenza tra Valore della Produzione e Costi Operativi della gestione caratteristica - verificatasi durante il periodo di interruzione o sospensione dei sistemi informatici.

Tale periodo ha inizio il giorno e l'ora in cui per la prima volta ha luogo l'interruzione o sospensione e ha termine il giorno e l'ora in cui è ristabilito il funzionamento dei sistemi informatici o sarebbe stato ristabilito dall'Assicurato o dal *Fornitore di Servizi* agendo con la dovuta prontezza. Tuttavia il periodo di interruzione prosegue la sua decorrenza senza soluzione di continuità nel caso in cui, nei sessanta minuti successsivi alla rimessa in funzione dei sistemi informatici, questi dovessero subire un'ulteriore interruzione o sospensione per le stesse cause che l'hanno provocata inizialmente.

La perdita di reddito indennizzabile è quantificata raffrontando il MOL del periodo di interruzione o sospensione con il MOL dell'analogo periodo nell'arco dei dodici (12) mesi immediatamente precedenti.

Nel calcolo della perdita di reddito indennizzabile non si tien conto di perdite dovute a fattori diversi da quelli del *Sinistro*. Qualora l'Assicurato o il suo *Fornitore di Servizi* non intervengano con la dovuta prontezza per rimettere in funzione i *Sistemi Informatici*, l'indennizzo sarà ridotto in proporzione al pregiudizio che ne derivi alla Società Assicuratrice.

Resta inteso che la Società Assicuratrice risponde della perdita di reddito per una durata massima di sessanta (60) giorni di interruzione, da conteggiarsi dopo lo spirare di un periodo di carenza di 12 (dodici) ore dal momento in cui ha inizio il periodo di interruzione.

I.2 - Costi supplementari

La Società Assicuratrice tiene indenne l'Assicurato dei seguenti costi supplementari incorsi nelle suddette circostanze:

1. le spese necessare e ragionevolmente sostenute dall'Assicurato nel corso del periodo d'interruzione al fine di minimizzare, ridurre o evitare una perdita di reddito;
2. i costi della perizia informatica, ossia le spese necessarie e ragionevolmente sostenute dall'Assicurato per ricercare l'origine o la causa di un attacco ai sistemi.

La Società Assicuratrice risponde dei costi supplementari a condizione che il loro ammontare:

a. sia maggiore dei costi che l'Assicurato avrebbe sostenuto se non si fosse verificata l'interruzione o la sospensione dei sistemi informatici
b. e non sia maggiore della perdita di reddito che l'interruzione o la sospensione avrebbe provocato.

J - E-CRIME (Garanzia opzionale)

(forma «losses occurring»)

La Società Assicuratrice si obbliga a tenere indenne l'*Assicurato* da qualsivoglia danno patrimoniale diretto derivante da Trasferimento Fraudolento di Fondi di cui l'*Assicurato* sia venuto a conoscenza per la prima volta durante il *Periodo di Assicurazione*.

Per "Traferimento Fraudolento di Fondi" deve intendersi: perdita di denaro o valori depositati in un conto presso un istituto finanziario che derivi da una fraudolenta istruzione per iscritto proveniente da un terzo verso tale istituto finanziario per via elettronica, telegrafica, cavo o telefonica, volta a pagare o consegnare denaro o valori da qualsivoglia conto detenuto dall'Assicurato presso tale istituto, senza la consapevolezza o il consenso del medesimo.

CR.3 Esclusioni

CR.3.1 Esclusioni applicabili a tutte le garanzie

Le garanzie delimitate in questo allegato non sono intese a coprire i *Sinistri* che si basino o abbiano origine da:

1. azioni od omissioni commesse dall'Assicurato con intenti dolosi. Tuttavia questa esclusione non si applica ad azioni od omissioni commesse dai dipendenti dell'Assicurato che agiscano al di fuori della disciplina aziendale;
2. violazione di norme di legge concernenti l'emissione, il possesso, la negoziazione o la vendita di titoli mobiliari, nonché da informazioni date ai portatori di tali titoli. Questa esclusione non si applica se la violazione è conseguente a un *Fatto Dannoso* previsto dalle garanzie prestate con questo allegato;
3. comportamenti commerciali sleali, ingannevoli o illeciti, pratiche contrarie alla libera concorrenza, posizione dominante, infrazione delle relazioni commerciali vigenti, violazione della normativa antitrust;
4. circostanze o fatti già conosciuti, o che potevano essere ragionevolmente conosciuti, dal Contraente o dall'Assicurato all'inizio del *Periodo di Assicurazione*;
5. danni materiali e danni immateriali conseguenti, come da definizioni 15 e 17 figuranti nella Sezione Prima della polizza; danni corporali (definizione 14 figurante nella Sezione Prima della polizza); pregiudizi morali subiti da *Terzi* a meno che non siano la diretta conseguenza di un *Fatto Dannoso* previsto dalle garanzie prestate con questo allegato;
6. fatti attinenti ai rapporti di lavoro dell'Assicurato con i suoi dipendenti di ogni ordine grado (ivi inclusi: licenziamento ingiustificato o illegittimo, discriminazione, molestie sessuali e/o morali, provvedimenti disciplinari abusivi, gestione di piani o fondi di previdenza o assistenza);
7. responsabilità inerenti alla carica di Amministratore o Consigliere di Amministrazione, ivi inclusi quelli indipendenti, di Direttore Generale o qualsiasi posizione parificata;
8. richieste di risarcimento avanzate da uno o più Assicurati nei confronti di uno o più Assicurati titolari della stessa agenzia;
9. richieste di risarcimento avanzate da una società o azienda nella quale l'Assicurato è detentore di una partecipazione maggiore del quindici percento 15%, ovvero presentate da qualsivoglia società (controllata, correlata o consorella), od

organizzazione o persona fisica che detenga oltre il quindici percento (15%) dell'Assicurato;

10. patti contrattuali, obbligazioni o garanzie, che impongano all'Assicurato il pagamento di penalità o gli conferiscano responsabilità maggiori di quelle previste per legge in assenza di tali patti contrattuali, obbligazioni o garanzie. Questa esclusione non si applica:
    a. agli obblighi assunti dall'Assicurato con le imprese assicurative per la gestione di contratti di assicurazione e dei relativi sinistri;
    b. alle penalità previste dalla garanzia F (*Penalità PCI-DSS*);
11. raccolta illecita di informazioni personali o di altre informazioni a carattere privato, attuata per volere dell'Assicurato o col suo consenso, oppure attuata senza ottemperare all'obbligo di permettere alle persone interessate di dare o negare l'autorizzazione a tale raccolta;
12. invio non sollecitato di telefonate, immagini, email, spamming, messaggi elettronici o di qualunque altro tipo di comunicazione;
13. spionaggio, intercettazioni telefoniche, registrazioni audio e video che contravvengano la legislazione in vigore, anche se commessi da un soggetto del cui operato l'Assicurato debba rispondere a norma di legge;
14. danno alla proprietà intellettuale di *Terzi*, in particolare:
    a) inosservanza, violazione, contraffazione, divulgazione, utilizzazione fraudolenta, o appropriazione indebita di brevetti, idee, diritti d'autore, segreti di fabbrica;
    b) furto o divulgazione non autorizzata di un *Dato Protetto* nell'ambito della garanzia Responsabilità Civile in caso di *Danneggiamento dei Sistemi*
15. acquisto, vendita o negoziazione di azioni, quote o altri titoli societari o alterazione di conti societari;
16. perdita, appropriazione indebita o furto di fondi, valori, titoli o altri beni di proprietà di *Terzi*, affidati all'Assicurato in deposito o custodia;
17. sconti, buoni acquisto, rimborsi, premi o qualunque altro beneficio accordato dall'Assicurato a *Terzi*, al di là di quanto dovuto per legge o per contratto a seguito di *Danneggiamento di Dati* o *Danneggiamento dei Sistemi*;
18. costo del personale e spese generali dell'Assicurato, compensi e onorari di professionisti e *Fornitori di Servizi*, che non siano stati previamente approvati dalla Società Assicuratrice, salvo quanto stabilito per le garanzie H (Ripristino dei dati) e I (Perdite patrimoniali);

19. applicazione del diritto o di procedimenti legali, giudiziari o amministrativi o di procedure di mediazione degli Stati Uniti d'America o di uno qualunque di tali Stati o del Canada;
20. restituzione o compensazione di prezzi, onorari o remunerazioni spettanti all'Assicurato per beni o servizi forniti o da fornire;
21. furto o smarrimento di attrezzature multimediali o di dispositivi mobili, contenenti dati in formato elettronico, a meno che tali dati non siano in un formato criptato;
22. esecuzione o fornitura di prodotti o servizi, salvo quanto disposto nelle garanzie B e C di questo allegato (Responsabilità civile - Responsabilità connessa ad *Attività Multimediali*);
23. costi sostenuti per apportare migliorie al *Sistema Informatico* per renderlo più efficiente di quanto fosse prima del verificarsi di un *Sinistro*, salvo il caso in cui la tecnologia utilizzata prima del *Sinistro* non sia più in uso;
24. costi da sostenere per soddisfare le regole di conformità a seguito di una decisione giudiziaria, arbitrale o amministrativa che disponga un'ingiunzione o un rimedio equitativo o un danno punitivo e le conseguenti limitazioni;
25. liberazione, dispersione, o propagazione di sostanze inquinanti; presenza o emanazione di amianto; formazione, sviluppo, presenza, emissione o propagazione di funghi;
26. pretese e richieste di risarcimento presentate da o per conto di qualsiasi autorità amministrativa di qualsiasi Stato, comprese quelle dell'Unione Europea, fermo restando che questa esclusione non si applica alla copertura di cui alla garanzia E (Procedimenti amministrativi) delle presenti Condizioni Speciali o al pagamento dei costi di notifica previsti dalla garanzia A.3 (Notifiche prescritte) delle presenti Condizioni Speciali;
27. danni che sorgono, o si supponga siano sorti, da guasto o interruzione di alimentazione ad una infrastruttura energetica o di telecomunicazione, di utenze pubbliche, di servizi satellitari o di servizi esterni di comunicazione, qualunque ne sia la causa, che fornisce tali servizi all'Assicurato, quando tale infrastruttura non sia sotto il diretto controllo dell'Assicurato;
28. guerra, guerra civile, invasione, ostilità (con o senza dichiarazione di guerra), ribellione, rivoluzione, insurrezione, colpo di Stato; sequestro, confisca, nazionalizzazione, requisizione, nonché distruzione o danneggiamento di beni, di

Sistemi Informatici o di *Dati Protetti*, per ordine di un'autorità pubblica o governativa.

CR.3.2 Esclusioni applicabili alla garanzia C

La garanzia C (Responsabilità connessa ad *Attività Multimediali*), quale delimitata in questo allegato, non è intesa a coprire le richieste di risarcimento e i *Sinistri* che si basino o abbiano origine da:

1. obbligazione reale o asserita di pagare diritti di brevetto o royalties, interessi dovuti a ritardo e relative penalità;
2. costi di ristampa, richiamo, ritiro o distruzione di contenuti multimediali e di attrezzature o dispositivi che li contengano;
3. iniziative di organismi collettivi o di organizzazioni, nazionali o estere, addette alla protezione e alla riscossione di diritti di proprietà intellettuale (UIBM, SIAE e enti analoghi);
4. taluno dei seguenti fatti reali o supposti:
   a. inesatta, inadeguata o incompleta descrizione dei prezzi di merci, prodotti o servizi;
   b. errata stima di costi o promesse di redditività;
   c. mancata conformità dei beni, prodotti o servizi alla qualità e alle prestazioni annunciate;
5. scommesse, concorsi, lotterie, giochi d'azzardo;
6. pretese avanzate da o per conto di fornitori indipendenti dell'Assicurato o da soggetti a lui associati in joint venture, in relazione alla proprietà dei diritti su contenuti multimediali o a servizi da essi forniti all'Assicurato.

CR.3.3 Esclusioni applicabili alla garanzia H e alla garanzia I

La garanzia H (Ripristino dei dati) e la garanzia I (Perdita di reddito), quali delimitate in questo allegato, non sono intese a coprire i *Sinistri* che si basino o abbiano origine da:

1. avaria o disfunzione delle infrastrutture o dei servizi di fornitura di energia elettrica o di telecomunicazione, che non siano sotto il controllo diretto dell'Assicurato;

2. incendio, esplosione, scoppio, inondazione, terremoto, maremoto, eruzione vulcanica, fulmine, vento, grandine, cedimento del terreno, calamità naturale, distruzione o danneggiamento provocato da interventi dell'uomo;
3. avaria di satelliti;
4. perdite risultanti da congiunture economiche o da sfavorevoli condizioni del mercato;
5. costi sostenuti dall'Assicurato per individuare e porre rimedio a errori e vulnerabilità dei software;
6. costi di sviluppo e ricerca sui programmi, i software e le applicazioni di cui all'ultimo comma della definizione (e) di questo allegato, e costi per la tutela della proprietà degli stessi.

CR.3.4 Esclusioni applicabili alla garanzia G (Cyber Extortion)

La garanzia G (Cyber Extortion), quale delimitata in questo allegato, non è intesa a coprire i *Sinistri* che si basino o abbiano origine da:

1. minaccia di sequestro di persone o di danno alla loro integrità fisica;
2. minaccia di deterioramento, appropriazione o trasferimento di cose diverse dai *Dati Protetti*, anche se tale minaccia sia connessa a una minaccia ai *Dati Protetti* o anche se la sua attuazione possa causare danneggiamenti, alterazioni, asportazioni, dispersione o trasferimento di tali dati;
3. minaccia di un Assicurato verso un altro Assicurato o verso il Contraente.

CR.3.5 Esclusioni applicabili alla garanzia J (E-Crime)

Per "Trasferimento Fraudolento di Fondi" non si intende, e quindi deve ritenersi esclusa, qualsivoglia perdita derivante da:

1. qualsivoglia atto ricompreso nella politica di antiriciclaggio e per la prevenzione dei reati societari dell'Istituto Finanziario;
2. provato (o presunto tale) atto fraudolento, disonesto, criminoso od omissivo commesso, o coinvolgente, una persona fisica rientrante nella definizione di Assicurato;
3. qualsivoglia perdita indiretta o consequenziale, di qualsivoglia natura;
4. danni punitivi, esemplari ovvero multe, ammende, penali o perdite di benefici fiscali;
5. responsabilità nei confronti di terze parti, ad eccezione per i danni direttamente connessi ad un Trasferimento Fraudolento di Fondi;

6. costi e compensi per assistenza legale o quelli sostenuti per la dimostrazione o la prova del Trasferimento Fraudolento di Fondi;
7. furto, smarrimento, distruzione di, accesso non autorizzato a, o uso non autorizzato di informazioni confidenziali, ivi incluso un PIN o un codice di sicurezza;
8. qualsivoglia manomissione, alterazione di strumenti di negoziazione, valori, codumenti;
9. qualsivoglia provato (o presunto tale) utilizzo di carte di credito o debito, addebuto, accesso a tali carte ovvero utilizzo di informazioni contenute in tali carte.

CR.4 Forma dell'assicurazione

Le garanzie B, C, E, F, sono prestate nella forma «claims made» così come definita al punto 12 delle Definizioni figuranti nella Sezione Prima della polizza, con retroattività illimitata se non diversamente indicato nella Scheda di Polizza. La copertura postuma ha durata di cinque (5) anni e resta disciplinata dall'articolo CS.1.D delle Condizioni Speciali della polizza.
Le altre garanzie disciplinate da questo allegato sono prestate nella forma «losses occurring» così come definita al punto 13 delle Definizioni figuranti nella Sezione Prima della polizza.

CR.5 Limiti territoriali

Le garanzie B e C sono operanti per *Fatti Dannosi* avvenuti in tutti i Paesi del mondo, ad esclusione degli Stati Uniti d'America e del Canada.
Le altre garanzie disciplinate da questo allegato sono operanti per *Fatti Dannosi* avvenuti nel territorio della Repubblica Italiana, dello Stato Città del Vaticano e della Repubblica di San Marino.

CR.6 Denuncia e gestione dei *Sinistri*

CR.6.1 Denuncia e gestione dei *Sinistri* rientranti nella garanzia A (Assistenza e gestione degli eventi)

In caso di *Sinistro* rientrante nella garanzia A, si applicano i seguenti disposti:

1. venuto a conoscenza di un incidente avvenuto o presunto, l'Assicurato deve darne immediato avviso al *Team di Pronto Intervento* tramite l'indirizzo email sinistri.cyber@cgpa.eu nella consapevolezza che quanto più è tempestiva l'attivazione del Team tanto più è efficace al fine di prevenire danni o di ridurne la gravità e ampiezza;

2. ricevuto l'avviso suddetto, il *Team di Pronto Intervento* prenderà contatto con l'Assicurato il quale sarà tenuto a fornire tutte le informazioni e documentazioni utili per la gestione del caso. I componenti del *Team di Pronto Intervento* risponderanno alle domande dell'Assicurato sulla procedura e gli forniranno le indicazioni necessarie per far fronte al *Sinistro*;
3. il *Team di Pronto Intervento* gestirà il caso con propri operatori o avvalendosi di esperti fiduciari e avvocati, indicati nell'Appendice Informativa che costituisce parte integrante del presente allegato, ai quali l'Assicurato dovrà fornire la propria collaborazione rispondendo prontamente ad eventuali richieste o quesiti nel corso degli accertamenti e sopralluoghi e dando accesso ai file e ai sistemi tecnologici;
4. l'avvocato, nominato dal *Team di Pronto Intervento* di comune accordo con l'Assicurato, verificherà insieme agli esperti fiduciari se, in base alle *Norme sulla Notifica della Violazione*, le circostanze richiedono che sia data la notifica prevista dal punto A.3 della garanzia A e redigerà il testo della comunicazione da inviare agli interessati, di cui l'Assicurato dovrà fornire tempestivamente nominativi e indirizzi;
5. ove necessario, il servizio di assistenza telefonica previsto al punto A.4 della garanzia A sarà attivato da un apposito *Fornitore di Servizi* nominato dalla Società Assicuratrice;
6. l'eventuale servizio di vigilanza internet o di monitoraggio del credito, di cui al punto A.5 (Vigilanza internet) della garanzia A, sarà prestato da un *Fornitore di Servizi* competente in materia, nominato dalla Società Assicuratrice;
7. in ogni caso, la Società Assicuratrice non risponde per l'operato e per eventuali responsabilità del *Fornitore di Servizi* o degli esperti fiduciari e/o avvocati nominati ai sensi della presente clausola.

CR.6.2 Denuncia e gestione dei *Sinistri* rientranti nelle garanzie diverse dalla garanzia A (Responsabilità civile, Responsabilità connessa ad Attività Multimediali, Danni all'immagine dell'Assicurato, Procedimenti amministrativi, Penalità PCI-DSS, Cyber Extortion, Ripristino dei dati, Perdite patrimoniali conseguenti a un Sinistro)

In caso di *Sinistro* che interessi taluna delle garanzie diverse dalla garanzia A, si applicano tutti i disposti dell'art. 5 delle Condizioni Generali di polizza, con le seguenti integrazioni o precisazioni.

1. La denuncia del *Sinistro* deve essere effettuata all'indirizzo email **sinistri.cyber@cgpa.eu** e contenere la descrizione del *Fatto Dannoso* che lo ha originato o possa originarlo e il pregiudizio che può derivarne.
2. In caso di *Minaccia di Estorsione*, se ne dovrà dare comunicazione alla Società Assicuratrice entro i cinque (5) giorni dalla data in cui l'Assicurato l'ha ricevuta.
3. Qualora l'Assicurato e la Società Assicuratrice non siano d'accordo sulla valutazione di un *Sinistro*, ciascuna delle parti nominerà un proprio perito; i due periti così nominati ne nomineranno un terzo. Se non vi è intesa sulla nomina del terzo perito, questo sarà nominato dal Presidente della Camera di Commercio di Milano dietro semplice istanza delle parti o anche di una sola di esse. Ciascuna delle parti sosterrà il costo del proprio perito e la metà del costo del terzo.
   Il compito dei periti è di determinare i danni e il loro ammontare, e non la validità della copertura assicurativa. In particolare, la partecipazione alla procedura peritale non compromette il diritto della Società Assicuratrice a declinare il *Sinistro* o a richiedere il rispetto delle clausole contenute in polizza e in questo allegato.

CR.6.3 Applicazione della franchigia

La franchigia stabilita nella Scheda di Polizza si applica anche ai costi per l'attività posta in essere dagli esperti informatici e/o legali chiamati a collaborare con il *Team di Pronto Intervento* relativamente alle garanzie prestate alla lett. A) Assistenza e gestione degli eventi

Qualora il pagamento dei predetti costi, o più in generale il pagamento di un *Sinistro*, sia anticipato dalla Società Assicuratrice, l'Assicurato si obbliga a rimborsare l'importo della franchigia alla Società Assicuratrice, senza contestazioni, dietro semplice dimostrazione dell'avvenuta anticipazione.

APPENDICE INFORMATIVA ALL'ALLEGATO N. 1

I SERVIZI A VOSTRA DISPOSIZIONE

La garanzia Cyber Risk creata da CGPA EUROPE mette a disposizione degli assicurati un **Team di Pronto Intervento** con il compito di gestire i rischi e di fornire l'assistenza necessaria a seguito di un'eventuale violazione dei dati o dei sistemi informatici, reale o anche solo presunta.

La presente Appendice Informativa descrive le caratteristiche delle garanzie prestate da CGPA EUROPE, delineando il processo di risposta ad una violazione dei dati o dei sistemi informatici, ivi comprese le indicazioni per l'Assicurato su come riferirsi al Team di Pronto Intervento.

Le garanzie prestate da CGPA EUROPE comprendono una gamma di servizi tra cui l'assistenza durante ciascuna fase dell'indagine e gestione di un sinistro cyber da parte del Team di Pronto intervento, costituito da professionisti in ambito privacy ed esperti tecnico informatici.

La telefonata o l'invio di un'email al Team di Pronto Intervento, al fine di notificare una violazione presunta o reale dei dati e/o dei sistemi informatici, comporta l'attivazione dei seguenti servizi:

INDAGINE INIZIALE E CONSULENZA

- Servizi legali
- Servizi di informatica forense

GESTIONE EVENTO

- Servizi di notifica (inclusa la notifica in territori al di fuori dell'Italia, se necessario)
- Call center
- Risoluzione evento e servizi di mitigazione
- Pubbliche relazioni e spese di gestione degli eventi

PER NOTIFICARE UN SINISTRO, INVIATE UN'EMAIL AL SEGUENTE INDIRIZZO:

sinistri.cyber@cgpa.eu

OPPURE CHIAMATE IL SEGUENTE NUMERO: 0532 1640054

SERVIZI DI INFORMATICA FORENSE

Laddove si richieda l'intervento di esperti informatici forensi per poter valutare l'impatto di un evento, forniremo servizi adeguati al fine di:

a. assistervi nel determinare se e in che misura sia necessario ottemperare con i requisiti di legge in materia di notifica;

b. se applicabile, fornire consulenza in relazione all'indagine svolta da un investigatore forense PCI (Payment Card Industry).

Tali esperti necessiteranno dell'accesso ad informazioni, files e sistemi ed è fondamentale fornire la massima collaborazione. Il Team di Pronto Intervento reperirà tali servizi informatici e vi metterà in contatto con i nostri esperti; vi preghiamo di non contattare direttamente gli esperti da noi selezionati, e che trovate di seguito, senza prima aver contatttato il Team di Pronto Intervento.

- *DiFOB*
  http://www.difob.it/
  +39 011 0438192
- *SECURE GROUP*
  https://www.securegroup.it/it/
  +39 011 0700900

SERVIZI LEGALI

IL TEAM DI PRONTO INTERVENTO

CGPA EUROPE ha voluto fornire ai propri assicurati un servizio dedicato alla gestione della violazione dei dati o dei sistemi informatici creando un'unità specifica con il compito di gestire questi eventi. Il Team di Pronto Intervento lavora in collaborazione con gli assicurati per esaminare e determinare la gravità dell'incidente, coordinando le risorse e i servizi di cui può aver bisogno l'assicurato per soddisfare i requisiti normativi, mantenere la fiducia del cliente e proteggere la sua reputazione. Il Team è a disposizione degli assicurati a prescindere da vastità, gravità o pregiudizio creato dalla violazione dei dati o dei sistemi informatici.

QUANDO NOTIFICARE?

L'assicurato è tenuto a contattare il Team di Pronto Intervento di CGPA EUROPE non appena sospetti che informazioni personali o dati confidenziali dei quali è responsabile, possano essere stati violati. Quanto prima viene notificato l'evento, quanto più il Team di Pronto Intervento può essere d'aiuto. **Occorre notificare a CGPA EUROPE l'evento prima di contattare qualsiasi fornitore di servizi** dato che sarà il Team di Pronto Intervento a guidarvi durante il processo di gestione e risoluzione dell'evento. Inoltre, seguirà l'assicurato durante il processo di selezione dei migliori esperti sulla base di quanto accaduto.

COME NOTIFICARE?

Inviare un'email a sinistri.cyber@cgpa.eu contenente le seguenti informazioni:

- ragione sociale dell'assicurato e numero di polizza;
- breve descrizione dell'evento;
- data di accadimento dell'evento (se nota);
- data di rilevamento dell'evento da parte della organizzazione a cui fa capo l'assicurato;
- contatto di riferimento interno all'organizzazione a cui fa capo l'assicurato che seguirà la gestione dell'evento.

Vi invitiamo a:

- non inviare email ad altri indirizii di posta elettronica al fine di notificare l'evento;
- non includere informazioni di carattere personale o di natura sanitaria.

Suggeriamo di uilizzare l'email come strumento di notifica. In alternativa è possibile notificare l'evento chiamando il seguente numero 0532 1640054 e fornire le informazioni sopra descritte.

COSA SUCCEDE A SEGUITO DELLA NOTIFICA?

Un membro del Team di Pronto Intervento risponderà entro il giorno lavorativo successivo all'invio della notifica.

Verrà organizzato un appuntamento telefonico per discutere dell'evento, assistervi nell'indagine e valutare i migliori servizi disponibili forniti in polizza. Suggeriamo di far partecipare alla conversazione telefonica coloro i quali, all'interno della organizzazione, saranno conivolti nella gestione dell'evento. Il Team di Pronto Intervento collaborerà con voi durante l'intera durata delle indagini al fine di coordinare la fornitura dei servizi necessari alla gestione dell'evento.

CYBER ESTORSIONE: I SERVIZI DISPONIBILI

Le Cyber estorsioni (dette anche "ransomware") costituiscono una minaccia comune condivisa da qualsiasi organizzazione produttiva. Il Team di Pronto Intervento è in grado di fornire un'assistenza puntuale grazie alla estesa esperienza nella gestione di tale tipologia di eventi. Se l'assicurato subisce un'attacco di questo tipo, sarà fornita la seguente assistenza:

- dialogo immediato con i dipendenti dell'assicurato per poter determinare una gestione adeguata della crisi;
- contatto rapido con esperti informatici forensi al fine di poter determinare se informazione personali o sanitarie siano state compromesse;
- contatto con esperti in grado di fornire assistenza tecnica per la cifratura dei dati, ripristino degli stessi o reperimento di bitcoin laddove decideste di pagare il riscatto.

Laddove l'evento dovesse richiedere la notifica dello stesso ai sensi di legge, saranno messi a disposizione una serie di servizi legali al fine di assistervi nell'indagine e gestione dell'evento. Il Team di Pronto Intervento reperirà tali servizi legali e vi metterà in contatto con i nostri esperti; vi preghiamo di non contattare direttamente gli esperti da noi selezionati, e che trovate di seguito, senza prima aver contatttato il Team di Pronto Intervento.

- *BTG LEGAL*
  http://lnx.btglegal.it/it/home/
  +39 02 30322 560
- *BIRD & BIRD*
  https://www.twobirds.com/it
  +39 02 30356 000

SERVIZI DI NOTIFICA E CALL CENTER

Il Team di Pronto Intervento assisterà l'assicurato durante il processo di notifica; collaborerà con la vostra organizzazione con il fine di individuare i dettagli della notifica e come coordinare tale processo unitamente ai consulenti legali. Inoltre, Il Team di Pronto Intervento aiuterà l'assicurato nella redazione di una lista di domande frequenti per gli addetti dei call center. Vi preghiamo di non contattare direttamente gli esperti da noi selezionati, e che trovate di seguito, senza prima aver contatttato il Team di Pronto Intervento.

- *EXPERIAN*
  https://www.experian.com/
- *BAKER GOODCHILD*
  https://www.bakergoodchild.co.uk/
- *EPIQ SYSTEMS*
  https://www.epiqglobal.com/en-gb

I VOSTRI OBBLIGHI

Al fine di garantire che i servizi sopra elencati possano essere forniti rapidamente ed adeguatamente, occorre che vi atteniate strettamente alle procedure elencate nell'Allegato n. 1 e nella presente Appendice Informativa. Vi chiediamo di riscontrare qualsiasi quesito o richiesta da parte del Team di Pronto Intervento o dei fornitori di servizi in maniera rapida e di stipulare i contratti necessari con i nostri esperti per la fornitura dei servizi sopramenzionati.

CGPA EUROPE non potrà essere chiamata a pagare i costi derivanti dal mancato riscontro rapido di risposte, informazioni accurate o approvazioni necessarie per la fornitura di servizi.