Siseco srl e l’avvocato Enrico Candiani hanno eseguito uno studio relativo alla normativa introdotta dal Regolamento numero 679/2016 dell’Unone Europea. La normativa è soggetta a mutevoli e varie interpretazioni da parte degli studiosi e delle autorità Nazionali dei vari paesi ed è al momento priva di giurisprudenza di guida. L’applicazione del GDPR deve essere intesa come forma di auto responsabilizzazione del Titolare, il quale solo è deputato ad assumere le responsabilità per quanto dichiara e valuta in merito al trattamento dei dati di cui è in possesso. Il presente lavoro rappresenta una interpretazione possibile della normativa, ma l"applicazione del GDPR è altamente specifica, e non tutti gli aspetti e le interpretazioni del GDPR sono ben definiti.

Di conseguenza, questo contenuto viene fornito solo a scopo informativo e quale strumento di ausilio ai Titolari al fine di venir guidati nella autovalutazione dei rischi di trattamento e non ha alcuna pretesa di esaustività e di completezza. In particolare, si sottolinea l’importanza fondamentale, ai fini di una corretta adesione ai principi del GDPR, della consultazione di un esperto-consulente che, oltre alla valutazione fornita del presente lavoro, possa esaminare gli infiniti aspetti che caratterizzano il trattamento dei dati in ciascuna singola unità imprenditoriale o professionale, che non possono in alcun modo venir sostituiti da un algoritmo o da una procedura standardizzata.
Siseco srl e l’avvocato Enrico Candiani pertanto Vi invitano, prima di assumere qualunque decisione definitiva in merito alla Vostra conformità alla normativa, a voler consultare un esperto del settore legalmente qualificato.
Siseco srl e l’avvocato Enrico Candiani inoltre Vi invitano alla integrale lettura di tutti i documenti informativi e guide contenute nel GDPR NAVIGATOR e ad ottemperare alle attività da compiere segnalate in calce al documento DPIA generato, in quanto trattasi di adempimenti formali e sostanziali imprescindibili ai fini dell’adeguamento al GDPR.
Siseco srl e l’avvocato Enrico Candiani non assumono alcuna responsabilità per eventuali violazioni o non conformità che dovessero venirvi contestate da qualunque autorità o da qualunque interessato, nel caso in cui non abbiate consultato un esperto qualificato prima di adottare le procedure e i documenti forniti dal presente prodotto, che hanno e devono avere esclusivo scopo di guida facilitativa e non rappresentano in alcun caso consulenza tecnica o legale.

Siseco srl e l’avvocato Enrico Candiani si riservano il diritto di modificare i contenuti del prodotto e delle note legali in qualsiasi momento e senza alcun preavviso.

Tutti i contenuti del prodotto sono riservati e protetti dalla normativa italiana sulla tutela dei diritti in materia intellettuale, il cui contenuto viene accettato dagli utenti, i quali si impegnano, altresì, a rispettarlo integralmente.

D.P.I.A.

Linee guida sulla valutazione dell'impatto sulla protezione dei dati (DPIA) e sull’analisi necessaria a determinare se il trattamento possa "comportare un rischio elevato" ai fini del regolamento 2016/679

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

FORMAZIONE E COMUNIONE SOCIETA' COOPERATIVA ONLUS

amministrazione@coopfoco.org

PIVA 01495820886

Aggiornato e stampa il 26/07/2018

Titolare ALESSANDRO BRULLO

Il presente documento rappresenta documento di autovalutazione dei rischi previsto dall'articolo 35 del regolamento Europeo numero 2016/679 (cosiddetto DPIA).
Il documento di valutazione consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli).
I contenuti minimi della DPIA sono specificati come segue all'art. 35, paragrafo 7 del regolamento:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il valore e il ruolo della DPIA sono altresì chiariti nel Regolamento all'interno del "Considerando" n. 84 nei termini seguenti: "Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio."
Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35 Regolamento, paragrafi 1 e 3-4), lo svolgimento non corretto di una DPIA (art. 35 Regolamento, paragrafi 2 e 7-9) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (art. 36 Regolamento, paragrafo 3, lettera e)) possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore alla citata soglia del 10 milioni di Euro.
È possibile utilizzare un'unica DPIA per valutare più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.
Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di

gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
L'articolo 35 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.
Sono considerate situazioni particolari di rischio quelle nelle quali il Titolare compie, nella sua organizzazione:

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche11 (Si veda il considerando 71 del regolamento: "in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato");
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 1012 (Si veda il considerando 75: "se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza").
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

L'autorità di vigilanza (Garante) ha inoltre individuato le seguenti categorie di titolari che svolgono attività a rischio (si vedano, per esempio, i considerando 75, 76, 92, 116).
I. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91 del Regolamento). A titolo esemplificativo si possono citare un istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio ovvero un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una società

che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.
II. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura: trattamenti finalizzati ad assumere decisioni su interessati che producano “effetti giuridici sulla persona fisica” ovvero che “incidono in modo analogo significativamente su dette persone fisiche” (art. 35 Reg. , paragrafo 3, lettera a)). Per esempio, il trattamento può comportare l’esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione.
III. Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o “la sorveglianza sistematica di un’area accessibile al pubblico” (art. 35, paragrafo 3, lettera c)). Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità. Inoltre, è talora impossibile per gli interessati sottrarsi a questa tipologia di trattamenti in aree pubbliche (o pubblicamente accessibili).
L’interpretazione del termine “sistematico” è la seguente:
• che avviene per sistema;
• predeterminato, organizzato o metodico;
• che ha luogo nell’ambito di un progetto complessivo di raccolta di dati;
• svolto nell’ambito di una strategia.
L’espressione “area accessibile al pubblico” va intesa nel senso di un luogo aperto alla generalità delle persone, per esempio una piazza, un centro commerciale, una strada, una biblioteca pubblica.
IV. Dati sensibili o dati di natura estremamente personale: si tratta delle categorie particolari di dati personali di cui all’art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all’art. 10. A titolo di esempio, si può citare un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati. Vanno comunque considerate talune categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili (nell’accezione comune del termine), in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici

dall’interessato ovvero da terzi, il che ne esclude la riservatezza o quantomeno ne fa desumere la possibilità che tale dato sia fruibile anche per altri scopi. Il criterio in oggetto può riferirsi anche a dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.

V. Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di “larga scala”, anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, occorre tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala:

- a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;
- b) volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;
- c) durata, o persistenza, dell’attività di trattamento;
- d) ambito geografico dell’attività di trattamento.

VI. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell’interessato.

VII. Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, che si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

VIII. Utilizzi innovativi di applicazioni note o applicazione di nuove soluzioni tecnologiche o organizzative. Si pensi alla associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via. Il regolamento chiarisce (art. 35, paragrafo 1, e considerando 89 e 91) che l’utilizzo di una nuova tecnologia, definito “in conformità con il grado di conoscenze tecnologiche raggiunto” (considerando 91), può comportare l’obbligo di condurre una nuova DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone.

IX. Tutti quei trattamenti che, di per sé, “impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto” (art. 22 e considerando 91). Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l’accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.
Il titolare deve consultarsi con il responsabile della protezione dei dati (RPD/DPO), ove designato (art. 35, paragrafo 2); tale consultazione e le conseguenti decisioni assunte dal titolare devono essere documentate nell’ambito della DPIA. Il RPD è chiamato anche a monitorare lo svolgimento della DPIA (art. 39, paragrafo 1, lettera c)).

Sulla base di queste premesse giuridiche, la redazione del documento di valutazione appare sempre opportuna al fine di poter documentare alle autorità di controllo e vigilanza l’avvenuta adozione delle misure minime richieste per una corretta valutazione della situazione di protezione dei dati nella propria Impresa.
In particolare, al fine di valutare i rischi e le modalità concretamente operative per la corretta protezione dei dati di terze parti, definiti ‘interessati’, si è proceduto alla valutazione dell’effettivo tipo di dati raccolti e trattati, del modo in cui detti dati vengono raccolti e trattati, dei metodi di conservazione custodia e protezione dei medesimi allo stato della valutazione, il tutto al fine di predisporre idoneo piano di iniziative finalizzate all’adempimento degli obblighi dettati dal citato regolamento per la protezione dei dati, altresì noto come GDPR.

Lo schema adottato è il seguente:
• descrizione del trattamento ->
• valutazione necessità e proporzionalità ->
• misure previste per dimostrare osservanza di proporzionalità e necessità ->
• valutazione dei rischi per diritti e libertà interessati ->
• misure previste per affrontare i rischi ->
• documentazione ->
• monitoraggio e revisione

Attraverso singole e specifiche domande previste e predeterminate sulla base delle disposizioni del Regolamento, si sono individuati i singoli punti critici nella gestione dei dati di terze parti, e si è altresì compiuta una valutazione globale di insieme al fine di comprendere la sussistenza o meno dei rischi esistenti, anche al fine, eventualmente, di predisporre idonea domanda all’Autorità Nazionale (Garante) qualora il complesso della situazione aziendale consigliasse

tale intervento.
Si sono individuati quindi in autovalutazione i criteri per l'adozione di un piano di interventi finalizzato a risolvere le singole criticità e il livello di criticità globale.
Si sono infine proposti i singoli tipi di intervento tecnico, contrattuale, concettuale necessari sul piano programmatico e operativo al fine di rispettare la disciplina e le previsioni normative di cui al Regolamento.

Le definizioni contenute nel presente documento sono conformi a quelle del Regolamento (articolo 4) e dunque:
Regolamento (GDPR) = Regolamento Europeo 2016/679 del Parlamento Europeo del 27.4.2016
dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
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;
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;
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati,

indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
Titolare del trattamento, o Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
Consenso dell'interessato, o Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni

relative al suo stato di salute;
Stabilimento principale:
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;
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;
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;
Gruppo imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
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;
Autorità di controllo o Garante: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento;
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; oppure
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;
Obiezione pertinente e motivata o Obiezione: 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;
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 ;
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.
Contitolare(Art 26 del Regolamento): Soggetto che riveste, al pari del Titolare, diritti ed obblighi congiunti a causa della struttora, organizzazione o modo di gestione dell'Impresa.
Responsabile per la protezione dei dati (RDP o RPO)(art. 37 del Regolamento): Soggetto nominato – fra persone dotate di specifica competenza tecnico-giuridica in ambito di tutela della riservatezza dei dati e del trattamento, anche in ambito di competenze informatiche – ad opera del Titolare e del Responsabile del trattamento ogni qualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento.
Documento di valutazione (Art. 35 del regolamento): Documento contenente la valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, da compiersi allorchè un tipo di trattamento prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, in modo che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Dati 'particolari' detti anche 'sensibili' (art 9 del regolamento): dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento

sessuale della persona. Il trattamento di questa categoria di dati su larga scala è consentito solo nel rispetto delle stringenti condizioni di cui all'articolo 6 comma 1 del regolamento.
Dati personali relativi a condanne penali e reati (art 10 del regolamento): il trattamento di questa categoria di dati su larga scala è consentito solo nel rispetto delle stringenti condizioni di cui all'articolo 6 comma 1 del regolamento.
Rischio: si intende qualunque tipo di evento in grado di compromettere i "diritti e le libertà" degli interessati, e va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.
Qualora, in base alla valutazione compiuta, si ritenga sussistano rischi per gli interessati derivanti dal trattamento dei dati, occorre preventivamente interpellare il Garante.

Il WP29 propone i seguenti criteri utilizzabili dai titolari di trattamento per stabilire se una DPIA, o una metodologia specifica di DPIA, comprenda un numero di elementi sufficienti a garantire il rispetto delle disposizioni del regolamento:
• descrizione sistematica del trattamento (art. 35, paragrafo 7, lettera a)):

° si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (considerando 90);
° sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;
° si dà una descrizione funzionale del trattamento;
° si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
° si tiene conto dell'osservanza di codici di condotta approvati (art. 35, paragrafo 8);

• valutazione di necessità e proporzionalità del trattamento (art. 35, paragrafo 7, lettera b)):

° si definiscono le misure previste per rispettare il regolamento (art. 35, paragrafo 7, lettera d) e considerando 90) tenendo conto di quanto segue:

» misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:

• finalità specifiche, esplicite e legittime (art. 5(1), lettera b));
• liceità del trattamento (art. 6);
• dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c));
• periodo limitato di conservazione (art. 5(1), lettera e));

» misure che contribuiscono ai diritti degli interessati:

• informazioni fornite agli interessati (artt. 12, 13, 14);
• diritto di accesso e portabilità dei dati (artt. 15 e 20);
• diritto di rettifica e cancellazione (artt. 16, 17, 19); diritto di opposizione e limitazione del trattamento (artt. 18,19, 21);
• rapporti con responsabili del trattamento (art. 28);
• garanzie per i trasferimenti internazionali di dati (Capo V);
• consultazione preventiva (art. 36);
• gestione dei rischi per i diritti e le libertà degli interessati (art. 35, paragrafo 7, lettera c):

° si determinano l'origine, la natura, la particolarità e la gravità dei rischi (v. considerando 84) o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati:

» si tiene conto delle fonti di rischio (considerando 90);
» si identificano gli impatti potenziali sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;
» si identificano le minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;
» si stimano probabilità e gravità (considerando 90);

° si stabiliscono le misure previste per gestire i rischi di cui sopra (art. 35, paragrafo 7, lettera d) e considerando 90);

• coinvolgimento dei soggetti interessati:

° si chiede consulenza al RPD/DPO (art. 35, paragrafo 2);

° si sentono gli interessati o i loro rappresentanti (art. 35, paragrafo 9), se del caso.

A tali criteri l'impresa intende col presente documento adeguarsi.

Il registro di trattamento.

L'articolo 30 del Regolamento stabilisce che i titolari di trattamento tengano, sotto la loro responsabilità, un registro delle attività di trattamento. La norma è purtroppo molto generica ed ampia e le interpretazioni sul punto sono le più disparate. Ai fini del presente documento di autovalutazione si ritiene di impostare una interpretazione prudente e ragionevole della norma stessa.

Il registro dei trattamenti è uno strumento sicuramente molto utile per mappare i flussi di dati all'interno dell'organizzazione di impresa ed è certamente in grado, se utilizzato ed aggiornato, di dimostrare in sede di eventuali ispezioni, una particolare attenzione del Titolare alla normativa sulla sicurezza dei dati.

Può dimostrarsi utile, ad esempio, indicare nel registro, se previsto dalle buone prassi aziendali, quali database contengono le informazioni trattate, quali software le processano, quali server sono coinvolti in tali trattamenti, arrivando persino a indicare quali profili sono autorizzati al loro trattamento.

Appare ad esempio molto opportuno scindere le diverse modalità di trattamento dei medesimi dati in base alle singole finalità. Così, ad esempio, i dati identificativi di un cliente saranno trattati quantomeno per due finalità diverse: a) al fine di adempiere al contratto fra l'impresa e l'interessato; b) ai fini fiscali. Quindi – essendo diverse le finalità di trattamento del medesimo dato, sarà bene prevedere nel registro che i dati utilizzati al fine a) vengano conservati il tempo necessario per adempiere alla finalità a), mentre al fine b) vengano conservati il tempo previsto dalle norme tributarie, ma adottando misure che impediscano – ad esempio – il trattamento sub a) quando il termine utile sia ormai scaduto.

Appare sicuramente utile indicare nel registro se il trattamento richiede un consenso e quando è stato raccolto (inteso come momento generale in cui ciò avviene, ad esempio, al momento del conferimento dell'incarico, oppure al momento della sottoscrizione del form da parte dell'utente online ecc), se l'informativa viene correttamente consegnata e quando, o qualunque altra informazione si possa ritenere utile.

Il registro dei trattamenti non è un documento destinato a rimanere fermo e immutabile. Al contrario, deve essere inteso come un vero e proprio strumento di lavoro, e come tale deve essere modificato e mantenuto aggiornato, e sempre attuale.

Per raggiungere questo scopo è fondamentale innanzitutto individuare, all'interno dell'organizzazione, i soggetti che hanno la più ampia visione delle attività di trattamento e

coinvolgerli nella redazione e aggiornamento del registro dei trattamenti, responsabilizzandoli sull'importanza di tale attività. È necessario renderli edotti dei vantaggi e del valore aggiunto che una gestione trasparente dei flussi di dati personali rappresenta per l'azienda.
Il registro dei trattamenti dovrebbe essere gestito in maniera centralizzata, garantendo l'accesso a tutte le persone coinvolte nel suo aggiornamento, evitando quindi la creazione di più copie fra loro non coordinate.
Non è individuato alcuno strumento vincolato per tenere detto registro, sicchè esso potrà essere un foglio excel, o persino un registro cartaceo. Ovviamente, in tal senso potrebbe esser preferibile, per strutture complesse di'impresa, l'adozione di strumenti informatici disegnati appositamente a questo scopo.
Alla luce della sussistenza dei presupporti, l'impresa ha deciso di dotarsi del registro di trattamento.

Il sistema sanzionatorio preveduto dall'art. 83 del regolamento prevede sanzioni fino a 10 milioni di euro o, se superiore, fino al 2 % del fatturato mondiale dell'impresa per le seguenti violazioni:
a) Agli obblighi del titolare del trattamento e del responsabile del trattamento di cui agli articoli:

I) 8 (Consenso dei minori)

II) 11 (Trattamenti che non richiedono l'identificazione dell'interessato)

III) 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita)

IV) 26 (Contitolari del trattamento)

V) 27 (Rappresentanti di titolari di trattamento o dei responsabili di trattamento non stabiliti nell'Unione)

VI) 28 (Responsabile del trattamento)

VII) 29 (Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento9

VIII) 30 (Registri delle attività di trattamento)

IX) 31 (Cooperazione con l'Autorità di controllo – Garante)

X) 32 (Sicurezza del trattamento)

XI) 33 (Notifica di una violazione dei dati personali all'autorità di controllo-garante)

XII) 34 (Comunicazione di una violazione dei dati personali all'interessato)

XIII) 35 (Valutazione di impatto sulla protezione dei dati)

XIV) 36 (Consultazione preventiva)

XV) 37 (Designazione del Responsabile per la protezione dei dati – RDP/DPO)

XVI) 38 (Posizione del responsabile della protezione dei dati)

XVII) 39 (Compiti del responsabile della protezione dei dati)

XVIII) 42 (Certificazione)

XIX) 43 (Organismi di certificazione)

del Regolamento

b) Agli obblighi imposti dall'organismo di certificazione

c) Agli obblighi imposti dall'organismo di controllo relativi ai codici di condotta (art 41 comma 4 Reg.)

Il sistema sanzionatorio preveduto dall'art. 83 del regolamento prevede sanzioni fino a 20 milioni di euro o, se superiore, fino al 4 % del fatturato mondiale dell'impresa per le seguenti violazioni:

a. Ai principi di base del trattamento di cui agli articoli 5, 6, 7, 9 del Regolamento

b. Ai diritti degli interessati contenuti negli articoli:

b.I.12 (Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato)

b.I.12 (Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato)

b.II.13 (Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato)

b.III.14 (Informazioni da fornire qualora i dati personali non siano ottenuti presso l'interessato)

b.IV.15 (Diritto di accesso dell'interessato)

b.V.16 (Diritto di rettifica)

b.VI.17 (Diritto alla cancellazione o diritto all'oblio)

b.VII.18 (Diritto di limitazione del trattamento)

b.VIII.19 (Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento)

b.IX.20 (Diritto alla portabilità dei dati)

b.X.21 (Diritto di opposizione)

b.XI.22 (Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione)

c. Ai trasferimenti illeciti di dati a destinatari di paesi terzi o organizzazioni internazionali

d. Alle norme adottate dallo stato nazionale

e. All'inosservanza di un ordine, una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo o il negato accesso ai dati in favore dell'autorità di controllo

La base legale del trattamento dei dati deve essere univoca per ciascuna finalità di trattamento. Pertanto, l'impresa adotta procedure idonee a separare, ove occorre, la raccolta del consenso su dati che non abbiano come base legale:

• Obbligo di legge o regolamento
• Il contratto con l'interessato ovvero l'esecuzione di un rapporto contrattuale con l'interessato
• Il legittimo interesse del Titolare
• La tutela di interessi vitali dell'interessato
• L'esecuzione di un compito di interesse pubblico (valido essenzialmente solo per le pubbliche amministrazioni).

E pertanto, quando siano raccolti e trattati dati non aventi come base legale uno dei casi di cui sopra, oppure non strettamente pertinenti ai casi suddetti, propone facoltativamente all’interessato il consenso al trattamento di dati aggiuntivi per finalità dichiarate nel modulo di informativa

Il titolare del trattamento ai sensi della normativa vigente è: SOCIETA' COOPERATIVA SOCIALE FORMAZIONE E COMUNIONE ONLUS. VIA G. MARCONI 32/A CHIARAMONTE GULFI RG. P.I. 01495820886 RAPPRESENTANTE LEGALE BRULLO ALESSANDRO, COD. FISCALE: BRLLSN75B12H163B

Il titolare è soggetto con sede nell’Unione Europea. Non necessita la nomina di Rappresentante

I contitolari del trattamento sono: Componenti del CDA BRULLO SALVATORE - BRLSVT66D24C612A PASTORELLO LUCIA - PSTLCU80C64H163A ANASTASI GIACOMO SALVATORE - NSTGMS73L26F061R

L'impresa utilizza software in contitolarità, il che rappresenta una situazione di rischio elevato. Ciascun utente diviene contitolare del trattamento. L'impresa pertanto adotta con i contitolari precise modalità di regolamentazione dell'accesso ai dati e di livelli di permission agli accessi ai data bases o agli archivi analogici. La documentazione di tali prassi viene allegata al presente

L'impresa effettua servizi di hosting e quindi occorre regolamentare in sede contrattuale il trattamento dei dati con chi richiede il servizio di hosting. In tale veste assume la qualifica di responsabile esterno del trattamento, salvo il caso specifico in cui, per contratto, possa assumere autonomamente decisioni in merito alle finalità e alle modalità di gestione dei dati, nel qual caso diviene altresì contitolare del trattamento.
L'impresa che offra servizio di Hosting deve disporre contrattualmente con i propri fruitori di servizio che, i medesimi, trattino i dati da loro raccolti conformemente alle disposizioni del Regolamento, con espressa previsione di risoluzione del contratto e cessazione del servizio in caso di violazioni della conformità al regolamento da parte dei fruitori del servizio di Hosting.

I responsabili del trattamento sono: DIRETTORI DI SEDE OPERATIVA PAOLA CULTRARO: CLTPLA75M63B428D MARIA PAOLA DISTEFANO: DSTMPL83P53H163S ISABELLA ODDO: DDOSLL73M41E974H MARIA RENDE: RNDMRA69T44D086W

I responsabili del trattamento devono esser assoggettati a specifiche direttive e obblighi contrattuali, nonché formati alla importanza e agli strumenti per la protezione dei dati ed alle modalità di trattamento.
I medesimi sono inoltre istruiti al fine di tenere, ove richiesto, il registro generale di trattamento dei Responsabili.
Con tutti i responsabili del trattamento DEVONO esser stipulati per iscritto contratti o istruzioni formali sulle modalità di trattamento.

Il personale addetto al trattamento dei dati deve esser assoggettato a specifiche direttive e obblighi contrattuali, nonché formato alla importanza e agli strumenti per la protezione dei dati ed alle modalità di trattamento. Attualmente il personale risultato formato: A - SI.
L'impresa pertanto deve prevedere:
• corsi di formazione del personale
• sistemi che impediscano al personale l'estrazione archiviazione, stampa o duplicazione non autorizzata di dati
• contrattualizzazione del rapporto con i dipendenti/collaboratori

L'impresa inoltre valuta con periodicità annuale l'opportunità di rinnovare percorsi di formazione.

E' possibile che il responsabile al trattamento deleghi a sub-responsabili. I sub-responsabili inseriti nella catena di comando aziendale devono esser assoggettati a specifiche direttive e obblighi contrattuali, nonché formati alla importanza e agli strumenti per la protezione dei dati ed alle modalità di trattamento.

L’Impresa tratta dati definibili come sensibili (salute, orientamento sessuale, credo religioso o politico o filosofico, sindacale, dati biometrici, sentenze penali di condanna - art. 9 comma 1 Regolamento e art. 10 del Regolamento). Gli interessati:
1. devono esser informati attraverso specifico comma inserito nello strumento di informativa del trattamento dati che verrà sottoposto agli interessati stessi e
2. devono prestare specifico consenso.
3. Tali dati, per loro natura, rendono necessaria l’adozione del registro del trattamento.
   In considerazione della delicatezza del trattamento, i medesimi dati sensibili
4. devono venir trattati unicamente da personale a ciò autorizzato specificatamente e pertanto gli strumenti informatici devono prevedere l’adozione di strumenti idonei a consentire la visione e il trattamento solo a personale selezionato preventivamente e non alla generalità del personale.

L’Impresa dunque entro il termine di inizio del trattamento o, se successivo, entro il termine di entrata in vigore delle disposizioni del GDPR adotta meccanismi di protezione dei dati sensibili che verranno suggeriti dal RPD-DPO e dai propri consulenti informatici.

5. Il trattamento è ammesso senza consenso per assolvere obblighi specifici anche contrattuali, nonchè per la tutela di interessi vitali
6. Qualora l’Impresa sia una ONLUS il trattamento è ammesso senza consenso per i propri membri o ex membri.
7. Il trattamento è ammesso senza consenso per dati resi pubblici dallo stesso interessato.
8. Il trattamento è ammesso senza consenso per esigenze di tutela di diritti in sede giudiziaria.
9. Il trattamento è ammesso senza consenso per motivi di interesse pubblico.
10. Il trattamento è ammesso senza consenso in ambito medico-sanitario.
11. Il trattamento è ammesso senza consenso per archiviazione storica o scientifica in modo aggregato.
12. I dati trattati devono venir assoggettati a copia di sicurezza ordinaria e di ridondanza protetti da intrusioni e con l’adozione di misure tecniche idonee ad impedire la distruzione o perdita anche fisica dei dati medesimi. Il ripristino dei dati eventualmente persi o eliminati deve poter avvenire nel ragionevole termine di 72 ore lavorative.

Non è previsto il trattamento di dati biometrici

L'impresa si trova in una o più delle situazioni per le quali deve nominare il Responsabile per la protezione dei dati (RDP/DPO). Ed in particolare: (C) Dati cosiddetti Sensibili, (E) Monitoraggio sistem. e regolare degli interessati

L'impresa non intende effettuare attività di videosorveglianza oppure effettua attività di videosorveglianza con modalità tali da non monitorare in modo sistematico gli interessati e non su larga scala. Pertanto, non necessita la nomina del RDP/DPO.

L'impresa esercita ed esegue attività di profilazione. Oltre alla raccolta del consenso e all'informativa, il titolare deve valutare i rischi connessi alla profilazione, in particolare i rischi per la sicurezza e libertà degli interessati, valutando il bilanciamento fra il proprio interesse alla profilazione e i diritti degli interessati. Deve inoltre venir predisposto specifico piano di sicurezza per la ipotesi di violazione dei dati così come profilati.
In caso di violazione o perdita dei dati profilati, va prestata particolare attenzione ed occorre segnalare entro 72 ore l'avvenuta violazione/perdita di dati, tenendo in considerazione in particolare:

• Tipo di violazione avvenuta (sottrazione, danneggiamento, perdita)
• Natura, sensibilità e volume dei dati personali
• Facilità di individuazione degli individui coinvolti
• Severità delle conseguenze per gli individui coinvolti
• Caratteristiche particolari di individui (ad esempio bambini, persone esposte)
• Numero di individui coinvolti
• Caratteristiche particolari del titolare.
L'attività di profilazione comporta un livello di rischio medio e pertanto si procede all'individuazione, con l'ausilio del DPO se nominato o dell'esperto di sicurezza informatica, all'adozione di adeguate modalità di protezione.

Ai fini della valutazione in merito ai criteri utilizzati per la profilazione, l'impresa segnala quanto segue: La profilazione dei dati personali avviene tramite software, denominato MTWEB, protetto da codice di accesso e password sulla base di profili di autorizzazione definiti dal titolare del trattamento dati. La profilazione dei dati viene esercitata solo per utilizzo aziendale interno e i dati elaborati non vengono forniti a nessun soggetto esterno all'organizzazione aziendale, tranne che per i casi previsti dalla Legge.

L'impresa non tratta dati definibili come 'critici' quali numeri di carte di credito, credenziali di accesso, indirizzi email se associati a password di accesso, numeri di conti correnti bancari, movimenti bancari o estratti conto anche in forma analogica.

Il Responsabile della protezione dei dati: BRULLO SALVATORE: cod. fiscale: BRLSVT66D24C612A - email: salvatorebrullo@coopfoco.org

La base legale del trattamento è o può essere, in base alle finalità perseguite dall'impresa, A Obbligo di legge o regolamento, B Contratto con interessato o esecuz. di contr., C Legittimo inter. titolare trattam. o di terzi, D Interesse vitale e urgente dell'interessato, E Consenso esplicito dell'interessato

Le finalità del trattamento sono Adempiere alle obbligazioni contrattuali quali vendita di beni e servizi; Adempiere ad un obbligo di legge o regolamento, fra cui quelle di natura tributaria (fatture, dichiarazioni fiscali, pagamento imposte), previdenziale (tutela salute dipendenti, adempiere a obblighi assicurativi e fiscali dei dipendenti o agenti o simili) o di ordine pubblico; Proporre servizi o beni all'interessato (ossia le attività precedenti alla conclusione di un contratto con terzi); Eseguire profilazioni a fine storico, scientifico, statistico; Tutela di diritti propri o di terzi in sede giudiziaria; Al fine di inviare periodiche comunicazioni

informative, didattiche, newsletter;

L'impresa ritiene, indipendentemente dalla sussistenza di specifico obbligo normativo, esser opportuna la redazione del documento di autovalutazione, in quanto tale documento è strumento fondamentale per programmare l'attività e valutare le criticità della propria organizzazione rispetto alle regole dettate dal GDPR, nonchè per documentare il tipo di analisi del rischio effettuata.

L'impresa tratta dati, senza raccolta del consenso, per legittimo proprio interesse al trattamento, avendo preventivamente valutato il bilanciamento dei propri interessi rispetto a quelli dei titolari.
A tal fine, si adotta come criterio di base la valutazione del diritto degli interessati a non ricevere comunicazioni non necessarie o non volute, a non veder trattati dati esorbitanti gli stretti interessi del titolare e per periodi eccessivi. Si dispone che eventuali dati trattati per proprio interesse legittimo siano comunque cancellati in tempi brevi e non appena divenuti potenzialmente obsoleti.

Gli interessati sono informati del loro diritto a presentare reclamo al Garante attraverso specifico comma inserito nello strumento di informativa del trattamento dati che verrà sottoposto agli interessati stessi.

I dati raccolti sono passibili di trasferimento all'estero: B Si, verso stati aderenti all'unione Europea
*B: Essendo previsto il trasferimento all'estero di dati, ma all'interno dell'Unione Europea, gli interessati devono: esser informati attraverso specifico comma inserito nello strumento di informativa del trattamento dati che verrà sottoposto agli interessati stessi
*C Essendo previsto il trasferimento di dati in paese esterno all'Unione Europea, occorre stipulare contratto con il soggetto terzo sito all’esterno della Unione Europea, che garantisca protezione e il trattamento dei dati in modo conforme al regolamento. A tal fine alcuni soggetti hanno aderito con protocolli di portata generale (Google, Amazon).
L'invio dei dati a paese terzo non UE deve venir sottoposto a verifica di adeguatezza del paese destinatario, sulla base di valutazioni compiute dalla Commissioone Europea.
Qualora non si sia regolamentato adeguatamente col terzo il modo di trattamento dei dati, la trasmissione è vietata.
E' in ogni caso vietato il trasferimento di dati a paese terzo anche su ordine dell'autorità giudiziaria del detto paese terzo, salvo accordi di cooperazione internazionale.

I dati sono raccolti o possono esser raccolti presso l' interessato. Occorre informare interessato PRIMA o CONTESTUALMENTE della raccolta attraverso specifico comma inserito nello strumento di informativa del trattamento dati che verrà sottoposto agli interessati stessi che contenga:

- dati del titolare e del rappresentante
- dati del responsabile protezione dati se nominato
- finalità e base giuridica del trattamento
- destinatari dei dati
- eventuale intenzione di trasferire dati all'estero
- durata del periodo di conservazione o criteri per determinare la durata
- diritto all'accesso, rettifica, cancellazione, opposizione al trattamento, portabilità
- diritto di revoca al trattamento se possibile salvo obblighi di legge
- possibilità di esporre reclami all'autorità (Garante)
- se i dati sono obbligatori per l'esecuzione di un contratto, o per legge e le conseguenze qualora il consenso non sia prestato
- se i dati sono o saranno oggetto di profilazione e, in caso affermativo, la logica della profilazione
- l'esistenza di processi decisionali automatici e il diritto dell'interessato a che le decisioni avvengano previo intervento umano.

L' Impresa prevede procedure, anche a mezzo meccanismi automatizzati, di richiesta agli interessati di conferma dell’effettiva corrispondenza dei dati trattati alla situazione aggiornata dei dati stessi. Possono esser adottate misure che prevedano che l’utente, con periodicità prefissata (esempio ogni 3 o 6 mesi), accedendo alla propria area riservata, debba necessariamente visionare i propri dati e modificarli se del caso o dichiarare che nulla è mutato. Il tutto con adozione di procedura informatica che consenta la registrazione della chiamata al server, il salvataggio del form e l’apposizione di marca temporale.

L’Impresa informa gli interessati, attraverso specifico comma inserito nello strumento di informativa del trattamento dati che verrà sottoposto agli interessati stessi, circa la durata della conservazione nel tempo o i criteri per determinare il tempo stesso (esempio: entro termini di prescrizione dei diritti, o per obblighi tributari).

L’Impresa raccoglie i dati degli interessati ed il loro consenso sempre in modo esplicito. La modulistica di raccolta, sia cartacea che elettronica, deve essere separata da ogni altra modulistica e chiara e di semplice individuazione. In caso di raccolta elettronica, occorre

adozione di procedura informatica che consenta la registrazione della chiamata al server, il salvataggio del form e l’apposizione di marca temporale.

L'impresa non applica di default alcun vincolo nei confronti degli interessati a prestare consenso al trattamento di dati al fine di concludere un contratto.

I dati sono raccolti per l'esecuzione di un contratto di cui gli interessati sono parte, e per tale finalità il trattamento è considerato lecito dal Regolamento senza necessità di raccolta del consenso. I dati verranno raccolti nel rispetto del principio di minimizzazione e quindi saranno raccolti e trattati i dati necessari per concludere ed adempiere al contratto o per adempiere gli obblighi di legge da ciò derivanti, quali, fra gli altri, eventuali dati fiscali per l'emissione di documentazione avente carattere tributario, o dati relativi agli strumenti, anche elettronici, per una idonea e rapida corrispondenza con gli interessati stessi. Gli interessati vengono informati, prima della raccolta, attraverso specifico comma inserito nello strumento di informativa del trattamento dati che verrà sottoposto agli interessati stessi, del fatto che il dato viene raccolto a tale fine, le finalità specifiche per cui viene trattato, e quali siano le conseguenze nell’ipotesi in cui il consenso, se necessario, non venga prestato. L'impresa inoltre provvede a separare l'eventuale consenso fra i dati indispensabili all’esecuzione del contratto (la cui mancata raccolta dovesse rendere impossibile l’esecuzione del contratto stesso) dai dati non a ciò necessari, e per i quali dunque è possibile il rifiuto totale o parziale al consenso da parte dell’interessato. Eventuali altre finalità saranno trattate e regolate separatamente.

I dati sono raccolti per adempimento di obblighi di legge. L'interessato è informato prima della raccolta attraverso specifico comma inserito nello strumento di informativa del trattamento dati di quale sia l’obbligo di legge in base al quale il dato è raccolto e trattato. A tal fine, oltre al modello generale di consenso, il Titolare provvederà a redigere ed allegare al presente documento di valutazione specifiche clausole di informativa relative a particolari ipotesi nelle quali l'impresa si può imbattere, quali, fra le altre, adempimenti relativi a obblighi di natura tributaria, previdenziale, di sicurezza dei luoghi di lavoro, di natura ambientale, relativi a normative antiriciclaggio e simili.

L'interessato dispone di diritto legale alla revoca del consenso prestato e viene dunque informato del suo diritto a revocare il consenso nei limiti in cui detto consenso possa venir revocato, e quindi restando esclusi i casi in cui il trattamento del dato in precedenza acconsentito sia divenuto obbligatorio per legge. In quest'ultimo caso, tuttavia, in caso di revoca del consenso, l'impresa valuta la sussistenza di propri diritti od obblighi alla conservazione del dato ma ne limita il trattamento unicamente al fine dell'adempimento degli

obblighi di legge o alla tutela dei propri diritti, anche nei confronti dell'interessato, eventualmente in via giudiziaria.

L'impresa può trattare e raccogliere materiale fotografico. L'interessato deve prestare specifico consenso al trattamento di detto materiale ed a tal fine si predispone apposito modello o clausola di consenso.

L'impresa può trattare dati di minori ultrasedicenni, ed in tal caso raccoglie validamente il consenso prestato da tali minori di cui, laddove possibile, verifica l'età reale. In ogni caso, l'impresa verifica che siano raccolti solo i dati strettamente necessari alle finalità per cui i dati vengono trattati.

Il consenso alla raccolta dei dati di minore di anni 16 deve essere raccolto ad opera del genitore/tutore/esercente la potestà

L'impresa già prevede prassi idonee a consentire agli interessati di accedere ai loro dati. Si provvede ad adeguare il testo nel modulo di informativa in favore dell'interessato. L'impresa inoltre predispone procedura idonea per consentire la risposta in tempi ragionevoli (massimo 30 giorni) in favore dell'interessato che richieda l'accesso ai propri dati.
L'impresa dispone che alla richiesta di accesso ai dati sia dato riscontro scritto, anche in via elettronica. Si dispone sia adottata procedura che fornisca all'interessato, fra l'altro, il dato inerente il periodo di conservazione dei dati e le garanzie per il caso di trasferimento dati all'estero, ma non le modalità di trattamento, in quanto non previsto dalla normativa. L'impresa valuta la possibilità di mettere a disposizione degli interessati una modalità di accesso ai dati mediante accesso da remoto automatico ai dati stessi, a mezzo piattaforma sicura e con credenziali che permettano la ragionevole identificazione degli interessati.

L'impresa ha già adottato procedure di identificazione dell'interessato che chieda l'accesso ai propri dati, e dispone di adeguare le procedure in modo da rispettare una corretta prassi di identificazione dell'interessato richiedente l'accesso o la modifica dei dati adottando metodi manuali o informatici in grado di fornire ragionevole certezza dell'identità del richiedente.

L'impresa non trasferisce dati a terzi

Quando le finalità per cui i dati sono stati raccolti dovessero cambiare, l'impresa provvederà a che l'interessato venga informato, in particolare mettendolo in condizione di esercitare il diritto all'opposizione al mutamento delle finalità.

L'impresa verifica e rende adeguate le procedure di rettifica dei dati già esistenti, adeguandole alle esigenze del Regolamento, ed in particolare provvede ad informare l'interessato del proprio diritto attraverso il modulo di informativa.

L'impresa verifica se le procedura esistente di oblio-cancellazione dei dati sia coerente con le esigenze della nuova normativa e adegua le procedure, i criteri di cancellazione ed il modulo di informativa all'interessato. Si provvede a individuare e attuare procedure che consentano la cancellazione dei dati anche in presenza di obblighi di conservazione di altra natura, se possibile (es: conservare solo dati fiscali ai fini tributari ed eliminazione di tutti i rimanenti dati; possibilità di eliminare tutti i dati dopo che siano superati i divieti alla cancellazione derivanti da obblighi di legge come quelli fiscali). L'impresa stabilisce di implementare, con un bilanciamento fra costi e disponibilità tecniche ed economiche, i propri processi in modo che i dati vengano cancellati automaticamente allo spirare dei termini individuati.

Il titolare, ad esclusione dei dati che debbono esser conservati per obbligo di legge, determina di cancellare i dati non necessari degli interessati entro: dati contabili e di natura fiscale 10 anni dall'interruzione dei rapporti contrattuali; dati contrattuali non necessari ai fini contabili e fiscali 2 anni dall'interruzione dei rapporti contrattuali; per tutti gli altri casi nei termini previsti dalle normative in vigore.

L'impresa verifica se le procedura di limitazione all'utilizzo dei dati preesistente sia coerente con le esigenze della nuova normativa e adegua le procedure e il modulo di informativa. In particolare si predispone un piano tecnico-operativo che preveda il 'parcheggio' dei dati e il non trattamento dei medesimi fino alla soluzione delle contese sul punto.

L'impresa verifica se la procedura preesistente di notifica all'interessato della cancellazione dei dati eseguita in autonomia dal titolare sia coerente con le esigenze del Regolamento e dispone procedura ed istruzioni affinchè la cancellazione sia preceduta da idoneo avviso agli interessati e adegua il modulo di informativa.

Il diritto alla portabilità dei dati configura per gli interessati la possibilità non soltanto di ottenere e riutilizzare i dati forniti a un titolare, bensì anche di trasmettere questi dati a un diverso fornitore di servizi (appartenente allo stesso o a un diverso settore di attività). L'impresa verifica se le procedura di portabilità dei dati preesistente sia adeguata rispetto alle esigenze della nuova normativa e adegua le procedure e il modulo di informativa.
L'impresa valuta altresì se, tenuto conto dei mezzi a disposizione e dei costi necessari per dar

corso a tale tipo di attività, appaia equamente bilanciato il diritto degli interessati rispetto agli oneri cui andrebbe incontro in caso di gravi difficoltà tecniche operative.

L'impresa verifica se la procedura preesistente di esercizio del diritto di opposizione sia coerente con le disposizioni del Regolamento e adegua procedure e modulo di informativa.

L'impresa svolge o prevede di svolgere invio di comunicazioni commerciali e newsletter. Pertanto provvede a raccogliere sempre specifico esplicito consenso all'invio di corrispondenza periodica o occasionale.

L'impresa raccoglie e tratta dati per loro natura o per modalità di raccolta e conservazione, immutabili. L'interessato deve venir informato della possibilità che i dati raccolti non possano venir mutati in alcun modo attraverso specifica comunicazione nel modulo di informativa.

L'impresa ha meno di 250 dipendenti e il Registro di trattamento è obbligatorio solamente se vengono trattati dati 'sensibili' (art 9 del regolamento) e/o attinenti a sentenze di condanna penale (art 10 del Regolamento). Può essere tenuto in forma scritta, manuale o elettronica. Si suddivide in due registri: il registro del titolare di trattamento, il cui contenuto è indicato appresso, ed il registro del Responsabile di trattamento, dal contenuto più ridotto in conformità all'art 30 del regolamento.

Contenuto del registro:
• I dati del titolare
• I dati del contitolare
• I dati del rappresentante del titolare
• I dati del responsabile della protezione dati
• Le finalità del trattamento
• La descrizione delle categorie di interessati e delle categorie dei dati personali
• Le categorie dei destinatari cui i dati sono stati o saranno comunicati
• I trasferimenti di dati verso altri paesi, con documentazione delle garanzie pertinenti
• I termini ultimi per cancellazione dati
• Descrizione misure di sicurezza adottate
• I responsabili del trattamento inoltre registrano le categorie di attività svolte per conto del titolare:
1. dati del responsabile del trattamento, o relativo rappresentante
2. categorie di trattamenti effettuati

3. i trasferimenti verso paesi terzi e relative procedure di sicurezza e garanzia
4. descrizione delle misure di sicurezza e organizzative adottate
Non essendone necessaria la tenuta in base al requisito del numero di dipendenti, l'impresa provvede a valutare la sussistenza di altre ragioni giuridiche al fine di decidere per l'adozione del registro stesso.

Sono previste procedure per il caso di violazione e/o perdita dei dati. Viene individuata apposita procedura tecnica per il ripristino dei dati perduti o violati nel minor tempo possibile. Si stabilisce che l'impresa effettui, anche attraverso il DPO se nominato, apposita segnalazione al garante entro 72 ore SE si suppone vi siano rischi per diritti e libertà degli interessati. Il contenuto della segnalazione sarà composto come segue:
• va segnalata una descrizione della violazione
• vanno indicati i dati del RDP/ DPO se nominati
• vanno descritte le conseguenze della violazione
• vanno descritte le misure adottate per proteggere i dati e contrastare le conseguenze della violazione
• vanno informati gli interessati SE c'è rischio elevato che li riguarda, ma non se sono state adottate misure di protezione sia prima che dopo la violazione e non se l'avviso agli interessati richiede sforzo spropositato (in quei casi basta un avviso su un quotidiano, ad esempio).

Sono previste misure di protezione dei sistemi informatici e dei dati. Vanno previste e adottate misure di protezione fra cui:
• misure di pseudonimizzazione, in presenza di dati critici quali dati bancari, carte di credito e simili, laddove trattati
• adozione misure tecniche per garantire integrità, disponibilità, resilienza dei sistemi, individuate nelle apposite procedure tecniche allegate e stabilite col responsabile informatico
• capacità di ripristino tempestivo dei dati in caso di incidente fisico o tecnico (backup attivo), individuate nelle apposite procedure tecniche allegate e stabilite col responsabile informatico
• procedure per test e verifica dell'efficacia delle misure tecniche adottate individuate nelle apposite procedure tecniche allegate e stabilite col responsabile informatico.
• Valutare in particolare i pericoli cui si espone l'interessato in caso di perdita, distruzione, modifica o divulgazione, accesso accidentale o illegale ai dati.
• adozione di sistemi di crittografia dei dati in presenza di dati 'ultrasensibili' trattati sistematicamente, secondo le apposite procedure tecniche allegate e stabilite col responsabile informatico

In Azienda esiste già una figura esperta in cybersecurity. Verranno predisposti corsi e manuali operativi da aggiornare con cadenze ragionate. Predisporre con essi formazione dei Responsabili del trattamento.

Disaster recovery dei dati. Sono già previsti meccanismi adeguati di ripristino dei dati a partire dalle copie di backup quotidiane o pluriquotidiane. L'impresa documenta con apposito piano le attività previste per il ripristino dei dati e del tempo massimo nel quale eseguire e rendere i sistemi nuovamente operativi.

Sistemi di bakcup o ridondanza. Sono già previsti meccanismi adeguati quali backup quotidiani o pluriquotidiani, backup di ridondanza in house e non, protezione dei sistemi di backup da intrusioni o disastri accidentali. Predisporre piano di ripristino dei dati e del tempo massimo nel quale eseguire e rendere i sistemi nuovamente operativi.

Sistemi anti intrusione. Sono già stati progettati e predisposti con ausilio di DPO/RDP e/o consulente di cyber security meccanismi adeguati, idonei a prevenire, bloccare e individuare intrusioni nei sistemi informatici aziendali. L'impresa provvede al loro aggiornamento allo stato dell'arte con cadenze adeguate all'andamento del rischio.

L'azienda utilizza computer o dispositivi portatili. La situazione è ad alto richio per definizione e pertanto occorre predisporre apposito piano e progettazione finalizzata alla protezione dei dati. In particolare la cifratura del disco e l’adozione di criteri di sicurezza per l’accesso al portatile

Al fine di comprendere le esigenze di riservatezza della clientela verranno consultati i clienti in merito al trattamento dei dati, mediante questionario dal quale trarre elementi relativi alle esigenze di riservatezza e standard che i clienti stessi richiedono nel trattamento dei dati.

Sono adottate tutte le procedure idonee per la corretta raccolta del consenso secondo le disposizioni del Regolamento ed in particolare secondo la seguente casistica:

Elementi che necessitano il consenso esplicito da parte degli interessati
• per l’invio di newsletter
• per l’esercizio di attività di e-commerce
• per l’utilizzo di procedure di valutazione automatica ai fini di concludere contratto con l’interessato

• per l’utilizzo a fini di marketing diretto
• per la profilazione per pubblico interesse
• per la profilazione per marketing indiretto
• per la profilazione ai fini di ricerca storica, scientifica o statistica
• per il caso di mutamento delle finalità del trattamento
• per il trasferimento dei dati a terzi
• per il trasferimento dei dati all’estero
• per il trasferimento dei dati al di fuori della UE
• per l’utilizzo di materiale fotografico
• per il trattamento di dati non indispensabili al fine di concludere un contratto
• per il trattamento di dati di minore
• per il trattamento di dati di minore di 16 anni (genitore)
• Occorre inoltre separare il consenso per dati indispensabili ai fini della conclusione di un contratto dai dati non indispensabili, in modo che l’interessato possa prestare consenso al trattamento dei primi ed eventualmente non al trattamento dei secondi

Sono stati consultati i dipendenti e collaboratori in merito alle modalità di trattamento dei dati loro affidati. E' stato individuato un rappresentante dei responsabili di trattamento che fornisca parere scritto sulle modalità ed esigenze dei responsabili stessi e che deve esser sentito per ogni aggiornamento del DPIA.

Gli elementi che necessitano l’informativa scritta in favore degli interessati sono:
• I dati del titolare o dei contitolari al trattamento
• I dati del rappresentante dell’impresa se previsto
• I dati del DPO/RPD se previsto
• Le categorie di dati raccolti
• La fonte da cui hanno origine i dati
• Delle finalità per cui i dati sono trattati
• Della base giuridica per cui si esegue il trattamento
• I destinatari dei dati
• In caso di mutamento delle finalità per cui il dato è trattato
• Il trattamento di dati immutabili
• L’utilizzo di procedure automatizzate per l’assunzione di decisioni circa la conclusione di contratti con interessato
• Il diritto dell’interessato ad ottenere intervento umano in caso di procedure automatizzate per l’assunzione di decisioni circa la conclusione di contratti con interessato

• In caso di profilazione per pubblico interesse
• In caso di profilazione per marketing indiretto
• In caso di profilazione ai fini di ricerca storica, scientifica o statistica
• In caso di dati trattati per obbligo di legge
• In caso di dati trattati per obbligo contrattuale
• In caso di dati trattati per far fronte ad obbligazione contrattuale
• Delle conseguenze – rispetto alla conclusione di un contratto – per il caso in cui il consenso sia negato dall'interessato
• Della durata nel tempo della conservazione dei dati o dei criteri con cui determinare tale durata
• Del metodo con cui saranno eliminati i dati al termine della durata prevista
• Della sussistenza del diritto alla opposizione al trattamento
• Della sussistenza del diritto alla portabilità dei dati
• Della sussistenza del diritto alla modifica dei dati
• Della sussistenza del diritto alla cancellazione dei dati (oblio)
• Della sussistenza del diritto alla limitazione del trattamento
• Della sussistenza del diritto alla rettifica dei dati
• Della sussistenza del diritto all'aggiornamento dei dati
• Della sussistenza del diritto di accesso ai dati
• Della sussistenza del diritto ad ottenere copia dei dati
• Della sussistenza del diritto a presentare reclamo all'autorità Garante
• In caso di trasferimento dei dati a terzi
• In caso di trasferimento di dati all'estero
• In caso di trasferimento di dati in paesi extra EU
Si provvede all'adeguamento della modulistica

La raccolta del consenso avviene in modo distinto da altri aspetti. I moduli di informativa ed i moduli di consenso devono esser sottoposti all'interessato separatamente rispetto a qualunque altro tipo di modulistica.

L'impresa, tenuto conto del settore merceologico di cui si occupa e della esposizione sui media tradizionali e non tradizionali, non è soggetta ad elevato rischio di attacchi informatici.

Al termine dell'attività di valutazione si è tenuto conto dell'equilibrio fra i diritti del titolare e quelli dell'interessato, ritenendo che il programma di adozione di misure di sicurezza adottato

mediante:

• Predisposizione di idoneo modello di informativa, suddiviso fra:

1. Informativa generale, messa a disposizione della generalità degli interessati sul sito internet aziendale e su una bacheca informativa aziendale
2. Informativa sintetica sottoposta singolarmente a ciascun interessato
3. Informativa specifica per il personale dipendente

• Predisposizione di idoneo modello per la raccolta del consenso. A tal proposito, il modello di informativa viene personalizzato in modo tale da consentire agli interessati di prestare il consenso separato fra i dati necessari al fine dell'espletamento delle finalità di base (ad esempio: per fornire i beni e servizi di cui l'impresa si occupa) da altri dati non indispensabili a tale fine ma utili per finalità diverse, quali comunicazioni commerciali, notizie, newsletter, profilazione.
• La adozione di misure di protezione dei dati a mezzo idonei strumenti informatici
• La adozione di misure di ripristino dei dati in caso di perdite o accessi accidentali
• La predisposizione di metodologia e prassi interna che consenta la separazione dei dati che debbono per obbligo di legge esser conservati a lungo termine, quali, ad esempio, quelli di natura fiscale, da quelli che possono invece esser oggetto di separata eliminazione (diritto all'oblio) in tempi ragionevolmente più brevi
• La adozione di idonea formazione al personale
• La nomina di RPD/DPO
• L'acquisizione di esperti di cybesecurity interno o in outsourcing
• L'adozione del registro di trattamento

rappresenti un idoneo punto di equilibrio fra gli interessi in gioco.

Essendo possibile che i dati oggetto di trattamento vengano trasferiti all'estero, si è specificatamente stabilito che detti dati potranno venir trasferiti in uno stato estero dell'unione Europea in base ad accordi assunti con il destinatario dei dati che si impegni al pieno rispetto del Regolamento, il quale, trovando piena applicazione in tutta l'Unione Europea, deve considerarsi norma fondante la liceità del trasferimento dei dati ai sensi dell'art. 45 comma 2 lettera a) del regolamento. Sarà di volta in volta verificato se il destinatario si sia adeguato spontaneamente alle normative Europee con provvedimento di carattere generale o contrattuale.

Ai fini del trasferimento in paesi esterni all'Unione Europea, oltre alla stipula di eventuali specifici contratti con il destinatario che lo vincolino al rispetto delle normative previste nel Regolamento, l'Impresa si impegna a valutare preventivamente se sussista un giudizio di

adeguatezza del paese destinatario, compiuto dalla Commissione Europea, di modo che il paese destinatario rispetti le condizioni di cui all'art. 45 comma 2 lettere a) (Stato di diritto, diritti umani, legislazione in materia di sicurezza e protezione dei dati) b) (esistenza e funzionamento di una autorità equiparabile alle autorità Garanti previste dal regolamento) e c) (assunzione di impegni internazionali vincolanti ai fini della protezione del trattamento dei dati) del regolamento.

Si è valutato altresì che sussistono allo stato i seguenti rischi per la sicurezza e la libertà delle persone:

- Il trattamento di dati particolari, detti altresì 'sensibili'
- In caso di perdita o cancellazione accidentale o tecnica dei dati
- In caso di circolazione delle informazioni a personale non strettamente deputato al trattamento

concludendo che occorra adottare le seguenti specifiche attività supplementari di sicurezza:

- Adottare sistematicamente attività di codifica o pseudonimizzazione dei dati di cui al paragrafo precedente, rispettivamente in presenza di trattamento di dati 'particolari' o 'critici'
- Adottare il registro di trattamento
- Nominare il DPO/RDP
- Nominare esperto di cyber security
- Adottare strumenti idonei ad impedire l'accesso fisico agli archivi di tipo tradizionale contenenti le versioni non informatiche dei dati citati
- Adottare criteri di permission all'accesso dei dati sulla base delle effettive strette necessità di trattamento, limitando la platea dei responsabili di trattamento e le loro funzioni

E stabilendo che tali misure vadano adottate prima dell'inizio del trattamento delle sopra citate categorie di dati.

Inoltre, in considerazione del fatto che l'impresa:

- Possa trattare dati di minori di anni 18 ma maggiori di anni 16
- Possa adottare nel tempo misure tecnologiche di nuova implementazione
- Debba trattare dati fra loro disomogenei nella durata di conservazione (ad esempio dati di natura strettamente fiscale rispetto a dati non indispensabili a tale fine)
- Possa avvalersi di dispositivi portatili
- Ed infine tenuto conto della possibilità concreta di violazione o diffusione accidentale dei dati si ritiene di dover in ogni caso stabilire che il presente documento di autovalutazione sia

assoggettato a revisione almeno una volta ogni dodici mesi o a cadenza inferiore in caso di importanti novità tecnologiche o del sopraggiungere di prassi o pareri delle autorità che suggeriscano una revisione del presente documento.

L’impresa ritiene infine di disporre che:

- I moduli di consenso e di informativa siano sottoposti ad esame e revisione con cadenza non inferiore a 24 mesi
- La valutazione degli strumenti di cyber security sia eseguita a mezzo personale specializzato con cadenza non inferiore a 12 mesi
- Sia predisposto un piano di verifica della tenuta ed efficacia delle misure di sicurezza adottate, da allegare al presente documento, documentando le verifiche eseguite periodicamente
- L’aggiornamento della formazione del personale avvenga con cadenza non inferiore a 24 mesi
- In caso di trasferimento di dati a terze persone sia comunque disciplinata la modalità di trasferimento e trattamento per via contrattuale
- In caso di trasferimento di dati a paesi non europei o organismi internazionali, sia previamente valutata la sussistenza dei requisiti di adeguatezza, da documentare per iscritto

Data **Luogo** **Firma**

Attività da compiere: regolamentare, a mezzo apposito contratto da allegare al fascicolo GDPR, i rapporti di gestione e trattamento dei dati fra i contitolari. Il relativo documento è

allegato al DPIA e ne fa parte integrante

Attività da compiere: regolamentare, a mezzo apposito contratto da allegare al fascicolo GDPR, i rapporti di gestione e trasmissione e trattamento dei dati forniti dal cliente cui si offre servizio di Hosting. Il relativo documento - tipo è allegato al DPIA e ne fa parte integrante.

Attività da compiere: regolamentare, a mezzo apposito contratto da allegare al fascicolo GDPR, i rapporti di gestione e trasmissione e trattamento dei dati forniti al responsabile esterno del trattamento. Il relativo documento - tipo è allegato al DPIA e ne fa parte integrante.

Attività da compiere: predisporre piano di formazione del personale e documentazione dello svolgimento dei corsi formativi, in sede interna o esterna. Il piano di formazione e la documentazione sull'effettivo svolgimento dei corsi formativi sono allegati al DPIA e ne fanno parte integrante.

Attività da compiere: regolamentare, a mezzo apposito contratto da allegare al fascicolo GDPR, i rapporti di gestione e trasmissione e trattamento dei dati per i quali il responsabile è autorizzato a subdelegare. Il relativo documento - tipo è allegato al DPIA e ne fa parte integrante.

Attività da compiere: predisporre, con l'ausilio del DPO se nominato e del responsabile informatico interno o esterno, un piano di individuazione e messa in sicurezza dei data bases contenenti dati sensibili. Tale documento, da tenere sempre aggiornato, è parte integrante del DPIA.

Attività da compiere: Poiché l'impresa tratta dati della tipologia prevista dall'art. 37 comma 1 lettere b e c del GDPR, la nomina del Data Protecion Officer è obbligatoria. Allegare al DPIA la copia dell'atto di nomina del DPO/RDP.

Attività da compiere: predisporre, con il supporto del DPO se nominato e con il responsabile della sicurezza informatica un piano che individui le logiche di profilazione, le finalità della

profilazione e, qualora la profilazione non sia anonimizzata, predisporre adeguato piano di protezione dei data bases di profilazione, adottando quantomeno criteri di pseudonimizzazione dei dati o, in caso di trattamento di dati sensibili o ultrasensibili, la crittografia. Allegare i documenti così prodotti al DPIA come parte integrante dello stesso.

Attività da compiere: avendo l'impresa stabilito di nominare il Dpo, si allega al DPIA l'atto di nomina nonché la notificazione della nomina all'autorità garante.

Piano d'azione in merito ai criteri adottati per il trattamento dei dati in base ai soli interessi legittimi. Il Considerando 47 del regolemento definisce 'interesse legittimo' la situazione che si verifica quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. Tale situazione viene considerata legitimo interesse al trattamento dei dati anche senza espressione del consenso. L'impresa tuttavia ritiene di adottare criterio di massima prudenza per il trattamento dei dati in base al proprio interesse legittimo - tenuto conto del la Legge 27 dicembre 2017, n. 205, G.U. n.302 del 29-12-2017 - Suppl. Ordinario n. 62 -commi da 1020 a 1024, che ha imposto una notifica preventiva al Garante qualora si trattino dati in formato elettronico sulla base dei soli interessi legittimi. In particolare, in base al Considerando 47 GDPR, Il trattamento dei dati per finalità di marketing diretto viene considerato legittimo interesse adottando il criterio del bilanciamento di interessi fra impresa e interessati. In conseguenza, l'impresa ritiene di poter trattare, sulla base del legittimo interesse, i dati a fine di marketing diretto unicamente se detti dati concernono soggetti già clienti, mentre adotta il criterio di prudenza ulteriore nei confronti di soggetti non clienti, nel qual caso si premura di ottenere il preventivo consenso degli interessati per la proposizione di proposte di marketing diretto. L'impresa considera trattati legittimamente i dati trattati in funzione della protezione contro le frodi, per misura di sicurezza, o il trasferimento di dati tra parti diverse della stessa azienda. L'impresa considera legittimo il trattamento di dati finalizzato: - alla verifica dell'età degli interessati; - alla valutazione del rischio; - all'esercizio del diritto di opposizione al trattamento. In questi casi, l'impresa considera legittimo il proprio interesse a mantenere indirizzo di posta elettronica dell'interessato per impedire l'invio di ulteriori comunicazione commerciali; - alla personalizzazione del sito web per migliorare l'esperienza dell'utente; - all' analisi web, verifica del numero di visitatori del sito, commenti, e simili; - alla comunicazione di reati all'autorità giudiziaria.

Attività da compiere: allegare documento nel quale - col supporto del DPO e dei responsabili informatici aziendali - si individuano le procedure, specie tecnico-informatiche, da adottare per consentire l'aggiornamento e la correzione dei dati, possibilmente in modalità automatica.

Attività da compiere: predisporre ed allegare modulo - tipo che integri il modello base di consenso informato, suddividendolo almeno nelle seguenti tipologie di trattamento e finalità: previdenziali-assicurative per agenti, dipendenti e collaboratori; sicurezza sui luoghi di lavoro; tutela ambientale; adempimenti ai fini delle normative antiriciclaggio, e altro che risulta dall'analisi della tipologia di adempimenti obbligatori per legge.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la messa a disposizione in favore degli interessati di modalità di accesso ai propri dati.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la identificazione degli interessati richiedenti l'accesso, la modifica, la cancellazione e ogni altro diritto concernente i dati.

Attività da compiere: predisporre e allegare modulo-tipo per la richiesta di consenso al mutamento delle finalità di trattamento

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la messa a disposizione, in favore degli interessati, di modalità di rettifica dei propri dati.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la messa a disposizione, in favore degli interessati, di modalità di cancellazione dei propri dati. Predisporre altresì allegato contenente la procedura adottata per procedere alla materiale cancellazione dei dati, sia analogici che elettronici, ed eventuali procedure di cancellazione automatica.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per consentire il 'parcheggio' dei dati in presenza di contenzioso in merito alla liceità o meno del trattamento e/o della cancellazione dei dati

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la preventiva comunicazione agli interessati dell'imminente cancellazione dei loro dati da parte del titolare.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la messa a disposizione, in favore degli interessati, di procedure informatiche idonee a garantire la portabilità dei dati in formato machine readable.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per la messa a disposizione, in favore degli interessati, di procedure idonee a garantire il diritto di opposizione al trattamento dei dati.

Attività da compiere: predisporre ed allegare documento contenente l'indicazione delle procedure adottate per garantire il ripristino dei dati, per la valutazione dei rischi inerenti la sospensione o riduzione della capacità operativa dell'impresa nonchè per i diritti e le libertà degli interessati in caso di perdita o danneggiamento dei dati, nonchè i modelli-tipo per provvedere alla segnalazione dei data breach al garante e agli interessati

Attività da compiere: predisporre e allegare documento, redatto con l'ausilio del DPO e del Responsabile informatico, contenente l' elenco delle procedure tecniche adottate per la protezione dei dati, diversificate in base al tipo di dati che vengono trattati (ordinari, critici, sensibili ecc.)

Attività da compiere: allegare nomina di responsabile di sicurezza informatica

Attività da compiere: Allegare programma di disaster recovery redatto con l'ausilio del Dpo se nominato e del responsabile per la sicurezza informatica

Attività da compiere: Allegare programma di esecuzione di sistemi di backup e ripristino nonché test di funzionamento periodico, redatto con l'ausilio del Dpo se nominato e del responsabile per la sicurezza informatica.

Attività da compiere: Allegare programma contenente l'adozione di misure anti intrusione, redatto con l'ausilio del Dpo se nominato e del responsabile per la sicurezza informatica.

Attività da compiere: Allegare programma contenente l'adozione di sistemi di protezione dei dispositivi portatili (Smartphone, Tablet, PC portatili ecc) redatto con l'ausilio del Dpo se nominato e del responsabile per la sicurezza informatica.

Attività da compiere: predisporre ed allegare modulo contenente la consultazione, ai fini della protezione dei dati, del rappresentante dei dipendenti.