



ASSIFACT

Associazione Italiana per il Factoring

Consiglio del 30 maggio 2018

**Punto 11 all' ODG
Varie ed eventuali**

**Allegato 11.2
Procedura Privacy (Aggiornamenti)**

PROCEDURA ASSIFACT

TUTELA DELLE PERSONE FISICHE RISPETTO AL TRATTAMENTO DEI DATI PERSONALI

STATUS	DATA
Emissione	
1° aggiornamento	27 Maggio 2003
2° aggiornamento	20 maggio 2004
3° aggiornamento	31 Marzo 2009
4° aggiornamento (adeguamento alla nuova normativa: Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati personali")	30 maggio 2018

Sommario

1	PREMESSE	3
1.1	SCOPO.....	3
1.2	DEFINIZIONI.....	3
1.3	FINALITÀ ASSOCIATIVE E AMBITO DI COMUNICAZIONE DEI DATI.....	5
1.4	PRESCRIZIONI D.LGS. 196/03.....	6
1.4.1	Notificazione (art. 37).....	6
1.4.2	Informativa (art. 13).....	7
1.4.3	Consenso (art. 23).....	9
1.4.4	Sicurezza dei dati (art. 31).....	11
2	RUOLI E RESPONSABILITÀ.....	12
3	ATTIVITÀ E ADEMPIMENTI.....	14
3.1	STRUTTURA ASSOCIATIVE (LOGISTICA E INFORMATICA) E SISTEMI DI SICUREZZA	14
3.2	TIPOLOGIE DI DATI TRATTATI, FINALITÀ E MODALITÀ DEL TRATTAMENTO / OBBLIGHI D.LGS. 196/03..	15
3.3	MISURE MINIME DI SICUREZZA E CONTROLLI.....	20
4	ALLEGATI.....	ERRORE. IL SEGNA LIBRO NON È DEFINITO.
	NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI	ERRORE. IL SEGNA LIBRO NON È DEFINITO.
	CONFERIMENTO INCARICO AL TRATTAMENTO DEI DATI – DIPENDENTI ASSIFACT ...	ERRORE. IL SEGNA LIBRO NON È DEFINITO.

1 Premesse

1.1 Scopo

Il presente documento ha lo scopo di:

- descrivere i principi della normativa vigente in materia di tutela delle persone fisiche rispetto al trattamento dei dati personali¹ e di obblighi a carico del titolare/responsabile del trattamento, con particolare riguardo ai fondamenti di liceità dei trattamenti e all'adozione delle misure adeguate di sicurezza;
- descrivere la tipologia di attività svolta da Assifact, i dati trattati e modalità del trattamento;
- definire, tenuto conto delle caratteristiche individuate al punto precedente, le regole di comportamento da applicare in tutti i processi associativi che prevedono il trattamento di dati per garantire che ciò avvenga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità dei soggetti interessati. Sebbene la definizione di "interessato", ossia del soggetto a cui è rivolta la protezione dei dati personali che lo riguardano, sia stata modificata a partire dal 2011 restringendo l'ambito soggettivo alle sole persone fisiche, rispetto alla formulazione originaria del Codice Privacy che includeva anche le persone giuridiche e ogni altro ente o associazione, l'Associazione adotta policy di più ampia tutela, nell'ottica della massima trasparenza nei confronti degli Associati. I trattamenti effettuati dall'Associazione sono sempre ispirati ai principi di coerenza con le finalità, correttezza, proporzionalità, sicurezza, riservatezza e liceità.

1.2 Definizioni

Le definizioni dei termini specifici inerenti il trattamento e la tutela dei dati personali sono contenute nell'art. 4 del RGPD, a cui si fa rinvio. Si riportano di seguito, per pronto riferimento, solo alcuni concetti chiave della normativa applicabili all'ambito associativo e le specifiche declinazioni con riferimento al medesimo ambito.

Ai fini del presente documento si intende per:

RGDP	REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
ASSOCIATO	<ul style="list-style-type: none">• società per azioni o comunque personalità giuridiche che esercitano direttamente o indirettamente in misura significativa ed in via continuativa l'attività di factoring;• soggetti che non esercitano direttamente o indirettamente l'attività di factoring ma perseguono in maniera prevalente

¹ Le presenti procedure accolgono le novità in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali introdotte dal Regolamento UE 2016/679 del 27 aprile 2016 e in vigore dal 25 maggio 2018 (di seguito RGPD) rispetto alle disposizioni previste dal D. Lgs. 196/2003 (c.d. Codice Privacy);

	finalità compatibili con quelle dell'Associazione (es. studi legali, società di consulenza, provider informatici del settore finanziario, ecc.)
INTERESSATO	Secondo il RGPD, l'interessato è la persona fisica cui si riferiscono i dati personali. Ai fini del presente documento, si intendono anche gli Associati, ferma restando l'obbligatorietà degli adempimenti di legge circoscritta alle sole persone fisiche.
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. Al titolare spettano pertanto le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
RESPONSABILE	ASSIFACT la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
INCARICATI	RESPONSABILE INTERNO: Segretario Generale In relazione alla definizione del D.Lgs. 196/2003, non ripresa ma non esclusa dal RGPD, gli incaricati sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Il RGPD fa riferimento a "persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile", figura del tutto assimilabile;
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	qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, la consultazione, l'elaborazione, l'adattamento o la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati

1.3 Finalità associative e ambito di comunicazione dei dati

L'Associazione Italiana per il Factoring (Assifact) è un soggetto apolitico e senza fini di lucro.

Le finalità associative sono previste dalla Statuto e il trattamento dei dati è funzionale al raggiungimento di tali scopi non di lucro diretti a diffondere la conoscenza "scientifica" del prodotto e del mercato del factoring, a interloquire con le istituzioni nella soluzione dei problemi interessanti il factoring e a tutelare gli interessi della categoria degli operatori del settore.

In particolare, l'Associazione si propone di svolgere attività di informazione, assistenza tecnica e consulenza a favore degli Associati; compiere e promuovere attività di studio e di ricerca riguardanti il factoring, anche mediante pubblicazioni e convegni; promuovere e favorire l'interlocuzione e il confronto su temi di interesse comune fra gli Associati o fra essi e altri Enti; collaborare con altri Enti, Associazioni, Istituzioni ed Organismi in genere, sia pubblici che privati, italiani o esteri, nella soluzione dei problemi interessanti il factoring; svolgere attività di indagine statistica o di produzione di risultati statistici riguardanti il mercato del factoring; svolgere in genere ogni attività utile per il conseguimento dei fini dell'Associazione.

Per dare concreta attuazione ai compiti e alle finalità istituzionali associative, Assifact sostanzialmente organizza e coordina l'attività di Commissioni Tecniche e dei Gruppi di Lavoro composti dai dipendenti dei propri Associati, mantiene contatti di collaborazione e di confronto con dipendenti e rappresentanti di enti e istituzioni, interloquisce con gli stakeholder del settore, organizza convegni ed eventi formativi inerenti il factoring, coinvolgendo ed invitando soggetti con cui si hanno regolari contatti per lo svolgimento delle attività statutarie, trasmette newsletter e documenti informativi sulle principali novità interessanti il settore o l'attività e le iniziative dell'Associazione.

In relazione questo e rinviando ai successivi paragrafi per una disamina dettagliata dei trattamenti effettuati, i dati personali raccolti e utilizzati dall'Associazione sono rappresentati principalmente dalla rubrica dei contatti, contenente i nominativi e i recapiti dei soggetti regolari interlocutori dell'Associazione. Si tratta pertanto di dati personali "comuni" non riconducibile, fatta eccezione per i dati necessari al rapporto di lavoro subordinato, alle categorie particolari e sensibili.

I dati sono trattati tramite supporto informatico o altra modalità, anche non meccanizzata, che consenta il conseguimento dei fini associativi previsti dallo Statuto sociale.

L'ambito di comunicazione dei dati trattati è principalmente costituito dagli Associati, nell'ambito delle attività istituzionali a cui i medesimi soggetti partecipano.

Per i soggetti esterni all'ambito degli Associati, non è prevista la comunicazione e la diffusione dei dati personali, fatto salva la comunicazione a soggetti terzi che per conto dell'Associazione provvedono all'espletamento di funzioni specifiche, strumentali e strettamente connesse all'espletamento di un servizio richiesto dall'interessato.

Maggiore dettaglio informativo è invece previsto per la raccolta di dati relativi agli Associati, che si ricorda, sono persone giuridiche e quindi escluse dall'ambito di applicazione del RGPD. Tali trattamenti, come si vedrà di seguito, hanno molteplici finalità, fra cui la realizzazione di studio e ricerche inerenti il mercato del factoring, anche e soprattutto tramite l'elaborazione di statistiche associative derivanti dall'aggregazione dei dati dei singoli associati. E' prevista la massima diffusione possibile, non solamente agli Associati, indipendentemente dalla fornitura dei dati secondo il principio di reciprocità, ma anche agli operatori non Associati e al pubblico interessato, delle informazioni relative al mercato del factoring rivenienti da indagini, sia occasionali che sistematiche e organizzate, realizzate principalmente tramite la raccolta di dati/informazioni presso gli Associati. Tali informazioni statistiche, patrimoniali, finanziarie ed economiche inerenti i singoli operatori sono però elaborate e diffuse esclusivamente in forma aggregata così da consentire il monitoraggio dell'andamento del mercato e dei principali trend ma non essere riferibili alle singole società e a specifiche combinazioni di prodotto / domanda / offerta.

1.4 Prescrizioni normative

1.4.1 Registro dei trattamenti (art. 30 RGPD)

Il Regolamento europeo sulla protezione dei dati personali prevede l'obbligo in capo a ogni titolare/responsabile di trattamento dati (fatta eccezione per le organizzazioni con meno di 250 dipendenti e che non trattano particolari categorie di dati) di tenuta di un **registro delle attività di trattamento** svolte.

Tale registro va tenuto in forma scritta anche elettronica a disposizione dell'Autorità di controllo e i contenuti minimi sono fissati dall'art. 30 RGPD.

Seppure facoltativo in talune particolari circostanze (se il titolare non effettua alcun trattamento di dati sensibili o relativi al casellario giudiziale), le autorità di controllo lo hanno fortemente raccomandato in quanto "parte integrante di un sistema di corretta gestione dei dati personali", "strumento indispensabile per ogni valutazione e analisi di rischio".

Ai fini associativi, la tenuta del registro, che è elaborato in formato word e archiviato tenendo traccia della cronologia degli aggiornamenti, è parte integrante delle procedura privacy, "contenitore" della mappatura dei trattamenti di dati personali svolti nella complessiva attività associativa, e riporta le seguenti informazioni prescritte dal RGPD:

- a) il nome e i dati di contatto del titolare e del responsabile del trattamento;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- f) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative, che devono essere adeguate al livello di rischio secondo le previsioni dell'articolo 32, paragrafo 1 RGPD.

1.4.2 Notificazione e violazione dei dati personali

Il RGPD ha abolito l'adempimento inerente la notifica preventiva dei trattamenti prevista dal Codice Privacy. In realtà, per Assifact la notificazione (art. 37 codice privacy) non era

più un adempimento obbligatorio già dalla revisione delle norme del codice privacy che circoscrivevano l'obbligo solo in alcuni casi espressamente previsti (es. trattamenti di dati genetici, biometrici, dati di geolocalizzazione, dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari, ecc.). Seppure non tenuta alla notificazione, ai sensi dell'art. 38 comma 6 l'Associazione doveva fornire a chi ne avesse fatto richiesta, salvo che il trattamento riguardasse pubblici registri, elenchi, atti o documenti conoscibili da chiunque, le informazioni contenute nel modello di notificazione predisposto dal Garante. Tali informazioni e tale adempimento è ora sostituito nel regolamento, dalla tenuta di un registro delle attività di trattamento di cui al paragrafo precedente (par. 1.4.1)

E' stata però introdotta la **notifica delle violazioni di dati personali** (data breach notification) ossia l'obbligo di documentare tutte le violazioni di dati personali (comprese circostanze, conseguenze e provvedimenti adottati) e, tempestivamente, di notificare all'Autorità di controllo e comunicare agli interessati le eventuali violazioni dei dati personali **che presentino un rischio per i diritti e le libertà degli interessati**. L'obbligo di notifica non è quindi generale ma è subordinato ad una valutazione di rischio da parte del titolare del trattamento.

La notifica va effettuata tempestivamente ossia entro 72 ore e comunque "senza ingiustificato ritardo".

Si evidenzia che, a prescindere dall'obbligo di notifica al Garante e di comunicazione agli interessati, il RGPD (art. 33 par. 5) sancisce l'obbligo in capo ai titolari del trattamento di documentare in ogni caso le violazioni di dati personali subite, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

In relazione alla natura dei dati trattati in ambito associativo, si ritiene che le uniche violazioni che possano configurare l'obbligo di notifica siano quelle relative ai dati dei dipendenti che, in quanto riferibili anche a categorie particolari di dati, possono comportare un rischio per i diritti e le libertà degli interessati.

Per le altre categorie di interessati, si è valutato improbabile che la divulgazione del nome e del recapito (indirizzo o email aziendale) di un individuo in circostanze ordinarie possa causare danni sostanziali ai diritti e alle libertà della persona.

In ogni caso, ai fini associativi, il Responsabile del trattamento segnalerà al Consiglio di Assifact tempestivamente ogni violazione subita, anche se non notificate all'autorità di controllo e non comunicate agli interessati.

1.4.3 Informativa (artt.12, 13, 14 RGPD)

L'informativa deve essere data, per iscritto o con altri mezzi anche elettronici, all'interessato nel momento in cui i dati vengono raccolti o entro un termine ragionevole, che non può essere superiore a un mese, se i dati sono raccolti presso terzi.

Gli interessati hanno, infatti, il diritto di essere previamente e analiticamente informati in merito alle caratteristiche del trattamento.

In particolare l'informativa deve contenere le seguenti informazioni:

- a) gli estremi identificativi del titolare del trattamento e, se designato, del responsabile del trattamento, con i relativi dati di contatto². Si includono i dati di contatto del responsabile della protezione dei dati, se nominato.
- b) le finalità del trattamento cui sono destinati i dati;
- c) la base giuridica per il trattamento dei dati (es. consenso dell'interessato, obbligo di legge, esecuzione di contratto, legittimo interesse del titolare a condizione che non prevalgano gli interessi e i diritti dell'interessato);
- d) le categorie di dati personali interessate;
- e) la fonte da cui i dati sono stati ottenuti, se raccolti da persona diversa dall'interessato, incluso se sono stati ottenuti da fonti accessibili al pubblico;
- f) la natura obbligatoria o facoltativa del conferimento dei dati;
- g) le conseguenze di un eventuale rifiuto di rispondere;
- h) il periodo di tempo, o i criteri per individuare tale periodo, durante il quale i dati saranno conservati;
- i) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza³;
- j) eventuale intenzione di trasferire i dati al di fuori dell'UE
- k) i diritti di base dell'interessato in materia di protezione dei dati personali, fra cui in particolare il diritto di accesso ai dati personali, di rettifica o cancellazione degli stessi e il diritto di revocare il consenso in qualsiasi momento;
- l) il diritto di presentare un reclamo all'autorità competente per la protezione dei dati personali;
- m) se applicabile, l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e la logica implicita, comprese le relative conseguenze.

Il regolamento prevede che l'informativa non vada fornita se e nella misura in cui l'interessato disponga già delle informazioni sopra elencate o se comunicare tali informazioni risultasse impossibile o implicasse uno sforzo sproporzionato (o nella misura in cui tale adempimento rischiasse di pregiudicare gravemente il conseguimento delle finalità del trattamento), oltre all'ipotesi in cui la richiesta dei dati derivi da un obbligo legale.

Infine, è opportuno ricordare che l'informativa va fornita all'interessato solo nel caso di raccolta dei dati dal titolare presso l'interessato stesso o presso terzi. Pertanto, seppure non esplicitamente previsto dal regolamento ma in linea con precedenti orientamenti del Garante Privacy, l'informativa non viene fornita in caso di invio spontaneo e volontario di dati e posta elettronica da parte dell'interessato e l'utilizzo dei dati è finalizzato a rispondere alle richieste pervenute:

- l'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi email associativi comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva. Il titolare fornirà l'informativa all'interessato solo nel caso di

² Seppure il regolamento non lo preveda, si ritiene di poter continuare ad applicare, in quanto non in contrasto, la previsione del D.Lgs. 196/03 che stabilisce che se vi è più di un responsabile, deve esserne indicato almeno uno, indicando dove o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili.

³ Il regolamento precisa che tali destinatari possono essere o meno terzi. Ciò significa che si include anche, come era espressamente previsto dal Codice privacy 196/03 responsabili o incaricati del trattamento.

ulteriori trattamenti specifici con finalità diverse rispetto a quella connessa alla fornitura dei dati;

- l'informativa non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Il titolare fornirà l'informativa all'interessato solo al momento del primo eventuale contatto successivo all'invio del curriculum.

Ai fini associativi, per alcune tipologie di trattamento, sembrerebbe applicabile la prima tipologia di esonero prevista dal RGPD ossia quella relativa ai trattamenti per i quali l'interessato conosce già le informazioni sostanziali sul trattamento. In ambito associativo infatti tale ipotesi potrebbe ricorrere per i soggetti operanti presso altri Enti, Associazioni, Istituzioni ed Organismi che hanno regolari contatti con l'Associazione in relazione ai meri dati di contatto che vengono raccolti per queste tipologie di interessati (nome, recapito email, ente/istituzione d'appartenenza, eventuale incarico aziendale), tipicamente forniti volontariamente dall'interessato stesso per le finalità istituzionali associative che sono note, al perimetro di trattamento dei dati esclusivamente "interno" e alle finalità di trattamento strettamente connesse all'attività istituzionale dell'Associazione di promuovere attività di studio e di ricerca riguardanti il factoring, favorire l'interlocuzione e il confronto su temi di interesse comune e collaborare con altri Enti, Associazioni, Istituzioni ed Organismi in genere nella soluzione dei problemi interessanti il factoring.

In ogni caso, per questi soggetti l'informativa non verrà fornita al momento della rilevazione dei dati e inserimento nell'archivio contatti dell'Associazione, essendo applicabile la regola prevista per l'invio facoltativo, esplicito e volontario dei dati personali da parte dell'interessato, ma nel caso di trattamento per finalità diverse da quelle istituzionali sopra citate o periodicamente a tappeto anche per verificare l'aggiornamento dei dati.

1.4.4 Consenso (art. 7 RGPD)

Ogni trattamento di dati personali deve essere supportato da idonea **base giuridica**. La principale base giuridica, salvo alcune espresse esenzioni previste dalla normativa, è rappresentata dal **consenso** che deve essere espresso dall'interessato preventivamente al trattamento dei dati da parte dell'Associazione e deve avere le seguenti caratteristiche:

- essere informato;
- richiesto con un linguaggio semplice e chiaro e facilmente visibile, accessibile e comprensibile;
- richiesto con chiara indicazione di tutti i motivi del trattamento;
- fornito per uno scopo specifico;
- fornito liberamente;
- essere esplicito, con particolare riferimento ai dati sensibili o a trattamenti automatizzati quali ad esempio la profilazione, e fornito tramite un atto positivo (ad esempio, mediante una firma su un modulo o una casella elettronica che la persona deve spuntare online);
- essere revocabile e tale possibilità deve essere portata a conoscenza dell'interessato (ad esempio, un link per annullare l'iscrizione alla fine di una newsletter elettronica).

Senza il consenso dell'interessato, il trattamento non è ammesso, a meno che non rientri nei casi di esclusione previsti dall'art. 6 del RGPD ossia quando il trattamento:

- a) è necessario per adempiere ad un **obbligo legale** al quale è soggetto il titolare;
- b) è necessario per dare **esecuzione a un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- c) è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un terzo;
- d) è necessario, sulla base dei principi / criteri sanciti dalla normativa⁴, per perseguire un **legittimo interesse del titolare** o di un terzo destinatario dei dati a condizione che non prevalgano gli interessi, i diritti e le libertà fondamentali dell'interessato. Il legittimo interesse del titolare può costituire base giuridica valida anche per eseguire ulteriori trattamenti sui dati rispetto a quelli per i quali i dati sono stati raccolti, tenendo conto di un nesso logico tra le varie finalità, del contesto in cui i dati sono raccolti, della relazione fra interessato e titolare del trattamento, della natura dei dati personali trattati e delle possibili conseguenze per l'interessato derivanti dall'ulteriore trattamento;

Il RGPD enfatizza il concetto di perseguimento di "interesse legittimo prevalente" del titolare, che in un'ottica di bilanciamento fra interessi del titolare e diritti e libertà fondamentali degli interessati rende possibile il trattamento in assenza di consenso. E' lo stesso titolare che valuta, in relazione alla natura dei dati personali, alle finalità per cui i dati sono stati raccolti rispetto alle finalità di ulteriori trattamenti e alle conseguenze possibili derivanti da ulteriori trattamenti, se non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

In ambito associativo, il legittimo interesse del titolare è rappresentato principalmente dalle finalità istituzionali statutarie di diffusione della conoscenza del prodotto e del mercato del factoring e di promozione e sostegno dell'interlocuzione e del confronto su tematiche di interesse comune fra gli Associati o fra essi e le Istituzioni / altri Enti (in un'ottica di pieno rispetto delle dinamiche competitive e di conformità alle normative per la tutela della concorrenza e del mercato). Per perseguire tale interesse legittimo, in linea generale e salva una disamina puntuale eseguita nei paragrafi successivi, i trattamenti di dati personali posti in essere:

- riguardano principalmente dati "comuni" di contatto relativi a soggetti che hanno contatti più o meno regolari con l'Associazione,
- in relazione ai quali tali soggetti possono ragionevolmente attendersi un trattamento, e
- non sono suscettibili di cagionare rischi o danni per i diritti e le libertà degli interessati, se non di remota possibilità e lieve entità.

Tipicamente, ai fini associativi, dovrebbe configurare interesse legittimo dell'Associazione il trattamento dei dati identificativi e di contatto dei membri delle Commissioni Tecniche /

⁴ La valutazione del bilanciamento fra interesse legittimo del titolare e tutela dell'interessato non è regolata dall'Autorità ma compete al titolare del trattamento sulla base anche di alcuni criteri forniti dal regolamento quali ad esempio ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento (l'interessato può ragionevolmente attendersi che abbia luogo un trattamento con finalità coerenti / pertinenti alla relazione), trattamenti strettamente necessari alla prevenzione delle frodi, sicurezza delle reti.

gdl dipendenti degli Associati in quanto il trattamento avviene nell'ambito del rapporto di associazione con l'Associato per la realizzazione degli scopi statuari e per l'ordinario funzionamento dell'attività associativa.

1.4.5 Sicurezza dei dati (art. 32 RGPD)

La principale novità introdotta dal RGPD riguarda l'approccio adottato che si basa sulla **valutazione del rischio e sull'adozione di misure organizzative e di sicurezza ad esso commisurate** anziché su una serie di prescrizioni minime previste dalla normativa, con l'obiettivo di responsabilizzare il titolare e responsabile del trattamento. Ciò significa che è demandato ai titolari / responsabili di valutare e decidere in autonomia, fermo restando lo spirito del regolamento e i criteri indicati, le modalità e i limiti del trattamento nonché le misure di sicurezza da adottare.

In relazione a ciò, l'art. 32 RGPD prevede appunto che il titolare del trattamento debba adottare le **adeguate misure di sicurezza** (il complesso delle misure tecniche, informatiche, organizzative, logistiche, procedurali di sicurezza che configurano il livello adeguato di protezione in relazione ai rischi), che gli consentono di trattare, custodire e controllare i dati oggetto del trattamento in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, o modifica dei dati personali, di accesso / divulgazione non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Tale autonomia decisionale si traduce in una serie di attività e valutazioni fatte a priori e dimostrabili che conducono a configurare le attività di trattamento adeguate al livello di rischio per i diritti e le libertà degli interessati. E' quindi necessario attribuire a ciascuno dei trattamenti che si intende porre in essere il relativo rischio. Se il trattamento presenta rischi elevati va effettuata una Valutazione d'impatto sulla protezione dei dati. Ai fini associativi, quest'ultima casistica non risulta ad oggi presente e, per la tipologia di attività svolta e di dati personali raccolti, sembra un'ipotesi assolutamente remota.

Le misure di sicurezza devono tener conto dell'evoluzione del contesto e dei costi di attuazione, della tipologia dei dati trattati e finalità del trattamento e del rischio (misurato dalla probabilità e della gravità) per i diritti e le libertà dell'interessato che può derivare dal trattamento. Pertanto, per stabilire il livello adeguato di sicurezza richiesto è necessario stimare il livello di rischio, attraverso la mappatura dei trattamenti effettuati, distinguendo in base a:

- tipologia del dato:
 - categorie particolari di dati (sensibili, giudiziari, genetici, sanitari, ecc.)
 - altri dati aventi carattere altamente personale quali dati relativi a rendimenti professionali, situazione economica, interessi personali, ubicazioni, ecc.
 - altri dati personali "comuni" (es. meri dati di contatto)
- strumenti impiegati nel trattamento:
 - strumenti elettronici o automatizzati
 - strumenti manuali o comunque non automatizzati
- continuità ed estensione dei trattamenti:
 - monitoraggio sistematico
 - trattamenti su larga scala

- combinazione dati o profilazioni
- finalità di utilizzo e ambito di comunicazione e diffusione
- rischi per i diritti e le libertà degli interessati

Come anticipato, a differenza della precedente normativa privacy, che forniva nel disciplinare tecnico allegato al codice privacy indicazioni specifiche sulle misure minime di sicurezza da adottare, il RGPD non fornisce sostanzialmente alcuna indicazione, fatto salvo alcune indicazioni di massima, se ritenute opportune:

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

In linea generale, le principali misure di sicurezza adottabili a livello associativo si traducono in:

- a) autenticazione informatica ossia insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- b) adozione di procedure di gestione delle credenziali di autenticazione (i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica);
- c) utilizzazione di un sistema di autorizzazione ossia di un insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- h) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

2 Ruoli e Responsabilità

Il *Titolare del trattamento* è l'Associazione Italiana per il Factoring (ASSIFACT).

L'Associazione ha sede legale e ubicazione degli uffici, ove sono custoditi e/o trattati i dati oggetto della presente procedura, in via Cerva 9 – 20122 Milano.

Il Consiglio di Assifact definisce, in linee generali, le finalità, l'ampiezza e le modalità del trattamento ed individua il ruolo delle persone preposte al trattamento, impartendo istruzioni, anche con riferimento al profilo della sicurezza.

Il Consiglio di Assifact delibera la nomina del Responsabile del trattamento, precisandone analiticamente poteri, compiti e funzioni.

Il *Responsabile del trattamento* (cd. Responsabile Interno) è individuato nella persona del *Segretario Generale* dell'Associazione, domiciliato per la carica presso la sede di Assifact in via Cerva 9. La nomina viene conferita con lettera scritta (vd. allegati).

In relazione alla struttura associativa, il Responsabile Interno del trattamento può ricorrere al supporto di soggetti terzi esterni per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, procedendo alla nomina, se ne ricorrono le condizioni e ai sensi dell' art. 28 RGPD comma 4, come *ulteriori responsabili del trattamento* (cd. sub-responsabili o responsabili esterni). Tale nomina va effettuata mediante un contratto o con l'inserimento di specifiche clausole contrattuali nel contratto di outsourcing.

Tenuto conto che l'Associazione non rientra nei casi previsti dall'art. 37 RGPD di designazione obbligatoria, valutate le finalità dei trattamenti, la natura sostanzialmente comune dei dati trattati e le dimensioni/struttura organizzativa associative, non si è ritenuto opportuno designare un Responsabile della protezione dei dati (RPD). L'Associazione infatti non tratta dati particolari (dati sensibili e dati giudiziari) su larga scala né effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

Il regolamento, diversamente dal Codice Privacy D.Lgs.196/03, non cita più la figura dell'"incaricato" del trattamento ma fa riferimento a "persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile", figura del tutto assimilabile e non incompatibile. Pertanto, ai fini associativi, i dipendenti dell'Associazione vengono nominati, mediante lettera scritta (vd. allegati), *Incaricati del trattamento*, in considerazione del fatto che, per l'espletamento delle proprie mansioni, vengono a conoscenza di dati personali dei soggetti che vengono in contatto con l'Associazione e ne effettuano il trattamento. Essi devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare e del Responsabile.

Medesima nomina è prevista per eventuali collaboratori esterni incaricati dall'Associazione per lo svolgimento di specifiche attività che generano trattamento di dati. (vd. allegati).

I dipendenti e gli eventuali collaboratori esterni incaricati di trattamenti di dati sono tenuti a mantenere la riservatezza sulle informazioni di carattere personale acquisite in ragione della propria funzione. L'inosservanza da parte degli incaricati al trattamento di dati delle disposizioni contenute nella presente procedura può comportare l'applicazione di provvedimenti disciplinari e/o sanzioni.

Come anticipato, in relazione alla struttura e dimensione organizzativa dell'Associazione, i dati trattati (v. paragrafo 3.2) possono essere comunicati anche a soggetti esterni che per conto dell'Associazione provvedono all'espletamento di mansioni specialistiche (paghe e contributi, contabilità, stampa e postalizzazione di materiale associativo).

I soggetti esterni, che vengono a conoscenza dei dati personali trattati dall'Associazione, ricevono dal Titolare e dal Responsabile tutte le indicazioni per il corretto trattamento dei dati comunicati nel rispetto del codice della privacy.

Al consulente esterno incaricato della funzione paghe e contributi, trattando i dati sensibili relativi ai dipendenti (es. assenze per malattia, gravidanza, ecc.), viene conferito contrattualmente l'al trattamento di tali dati (da valutare in relazione al grado di autonomia e ampiezza delle attività svolte, se configuri il ruolo di titolare autonomo o di responsabile esterno, limitatamente al trattamento dei dati ad esso attribuito).

In conformità alla disciplina in materia di sicurezza e igiene del lavoro, l'Associazione ha nominato il medico competente in materia di igiene e sicurezza dei luoghi di lavoro per la sorveglianza sanitaria obbligatoria e la tutela dell'integrità psico-fisica dei lavoratori. Anche il medico competente è delegato contrattualmente al trattamento dei dati inerenti la sua funzione in qualità di titolare autonomo.

In relazione agli accertamenti preventivi e periodici sui lavoratori che il medico competente effettua ai sensi della normativa sicurezza e igiene del lavoro, egli istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio che custodisce presso la propria sede, assicurando il rispetto del codice privacy. Alle predette cartelle l'Associazione non può accedere, ricevendo dal medico competente solo la valutazione finale circa l'idoneità del dipendente (dal punto di vista sanitario) allo svolgimento delle mansioni attribuite.

Il consulente esterno a cui sono affidati la funzione di manutentore del sistema informatico e il servizio di hosting e assistenza su applicativi internet, ossia il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo degli elaboratori, di assistenza Tecnico/Sistemistica Hardware, di consentirne l'utilizzazione e di monitorare l'adozione e l'adeguatezza delle misure di sicurezza, di gestire ed ospitare il sito internet Associativo, viene incaricato per iscritto con elencazione analitica dei compiti che gli sono stati attribuiti (da valutare in relazione alla possibilità o meno di accedere ai dati, al grado di autonomia e ampiezza delle attività svolte, se configuri di responsabile esterno limitatamente al trattamento dei dati ad esso attribuito).

Assifact, in qualità di Titolare, vigila sul rispetto delle istruzioni impartite e sul rispetto delle disposizioni della Legge Privacy da parte del Responsabile.

Il Titolare e il Responsabile vigilano altresì sull'osservanza di quanto sopra da parte degli incaricati.

3 Attività e adempimenti

3.1 Struttura associative (logistica e informatica) e sistemi di sicurezza

Gli uffici associativi, ove i dati sono custoditi e trattati e gli incaricati svolgono l'incarico assegnato, non sono aperti al pubblico.

L'accesso ai locali da parte di personale non dipendente è tipicamente circoscritto alle riunioni degli organi associativi e delle commissioni tecniche, previa formale convocazione. E' possibile accedere agli uffici associativi solo previa identificazione personale e in presenza del personale dipendente.

I locali sono protetti da un sistema di allarme antintrusione; sono dotati di porta blindata e di sistemi di bloccaggio delle tapparelle.

L'Associazione si è dotata di una cassaforte costruita in materiale ignifugo per la custodia dei valori, dei principali documenti associativi in originale (es. atto costitutivo), dei libri sociali e documenti relativi al personale (libri matricola, fogli presenza, libro paga e libro retribuzioni).

Il sistema informatico è composto da personal computer (desk top), in dotazione ai dipendenti dell'Associazione, collegati in rete locale tramite un sistema di cablaggio strutturato fonia/dati (LAN Ethernet), e da un server dedicato all'organico associativo, che permette di concentrare servizi di condivisione classiche (file e stampanti), backup automatici, DNS e la gestione delle credenziali di sicurezza per l'intero sistema, garantendo al tempo stesso un'elevata disponibilità grazie al dimensionamento ridondante delle parti critiche della macchina ospite (alimentazione, dischi, memoria).

L'Associazione dispone anche di una postazione pc mobile (laptop stand alone utilizzata, generalmente non collegata in rete, per lo svolgimento dell'attività delle Commissioni o attività didattiche).

L'accesso ad internet, tramite un collegamento ADSL/fibra, viene erogato da un provider di livello nazionale (Telecom/TIM) che fornisce i servizi base per la navigazione. Le politiche di firewalling di base sono predisposte direttamente dall'Associazione, con applicazioni ad hoc. L'Associazione dispone anche di due access point wireless, uno ad esclusivo uso interno ed uno wi-fi guest.

Il Mail Server è fornito da Assocons srl che si appoggia ad un provider internazionale (Aruba Business).

Il Web Server è fornito da Assocons srl che ospita il sito Assifact (sia l'area pubblica che l'area riservata) sui propri Server collocati in una web farm internazionale (Aruba Business).

L'accesso ai singoli pc è possibile tramite userid e password personalizzate e riservate ai singoli utenti.

Su ogni postazione di rete (server compreso) è installata una suite antivirus completa ed efficace, con automatizzazione degli aggiornamenti.

L'Associazione dispone di un sito associativo, composto da una parte pubblica ed una parte riservata agli Associati accessibile tramite userid e password personalizzate (rilasciate dall'Associazione secondo procedure definite e con aggiornamenti periodici), ospitato sui web server di Assocons Srl. La parte pubblica del sito associativo è creata e distribuita tramite Wordpress ed è gestita e aggiornata dal personale dipendente autorizzato dell'Associazione. La parte riservata è progettata e realizzata da Assocons srl, che ne cura la manutenzione, ed è alimentata nei contenuti dal personale dipendente autorizzato dell'Associazione, che è incaricato anche della gestione delle utenze.

I documenti in formato elettronico sono archiviati sul server e viene effettuato giornalmente il back up di sicurezza.

I documenti in formato cartaceo sono archiviati, in base a criteri definiti, in faldoni e classificatori e sono conservati in armadi e archivi a cui ha accesso il solo personale dipendente.


3.2 Tipologie di trattamenti e Adempimenti normativi

In relazione alla specifica operatività di Assifact, si riportano di seguito le categorie di interessati coinvolte, le tipologie di dati trattati, le finalità del trattamento e l'ambito di utilizzo.


Per ciascuna tipologia di dato / trattamento si individuano le prescrizioni della legge privacy.


Si evidenzia che i dati personali sono forniti direttamente dall'interessato. Fanno eccezione i dati personali relativi ai dipendenti degli Associati Assifact (membri degli Organi Associativi, delle Commissioni Tecniche e Gruppi di lavoro Assifact, Responsabili Statistiche, ecc.) per i quali i dati possono essere forniti ad Assifact, oltre che direttamente dall'interessato, anche dagli Associati Assifact in qualità di datori di lavoro, per consentire la partecipazione ai lavori associativi nell'ambito dell'ordinario svolgimento delle attività istituzionali stabilite dallo Statuto.

Dipendenti

 Nome, cognome, indirizzo, data di nascita, codice fiscale, altri dati identificativi equivalenti e coordinate bancarie sono necessari per la costituzione e l'esecuzione degli obblighi derivanti dal contratto di lavoro subordinato. Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per l'esecuzione degli obblighi contrattuali e in adempimento a obblighi di legge, i dati potranno essere comunicati a soggetti terzi esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. Consulente per paghe e contributi, Istituto creditizio per pagamento retribuzione e altre competenze, Pubbliche Amministrazioni, Casse di previdenza e assistenza, ecc.).


Obbligo di INFORMATIVA

 **No obbligo di CONSENSO** perché i dati sono raccolti in base ad un obbligo di legge, il trattamento è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato e perché la comunicazione è funzionale all'esecuzione del contratto.

 Dati di natura particolare quali dati sensibili (dati sanitari e stato di salute) o relativi ai provvedimenti di cui all'art. 686 c.p.p. (casellario giudiziale) o appartenenza sindacale sono necessari per l'esecuzione del rapporto contrattuale e per l'adempimento di obblighi previsti dalla legge. Il trattamento di questi dati è svolto con strumenti manuali ed anche con l'ausilio di mezzi elettronici o comunque automatizzati ed è effettuato per la gestione del rapporto di lavoro. Per l'esecuzione degli obblighi contrattuali e in adempimento a obblighi di legge, i dati potranno essere comunicati a soggetti terzi esterni, pubblici o privati, che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. Consulente per paghe e contributi, Pubbliche Amministrazioni, Casse di previdenza e assistenza).


In relazione agli accertamenti preventivi e periodici sui lavoratori che il medico competente effettua ai sensi della normativa sicurezza e igiene del lavoro, egli istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio che custodisce presso la propria sede, assicurando il rispetto del codice privacy.

Obbligo di INFORMATIVA

 **No obbligo di CONSENSO** in quanto il trattamento (art 9 comma 2 lettera b) è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi


del diritto degli Stati membri. L'Associazione valuta comunque opportuno evidenziare al dipendente il trattamento di tali dati e richiedere esplicito consenso.

Associati

 Denominazione o Ragione Sociale, indirizzo e telefono, altri dati identificativi (es. CF, P.IVA) e riferimenti bancari sono necessari ai fini dell'iscrizione all'Associazione e per l'adempimento degli obblighi contabili e fiscali. Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per l'esecuzione degli obblighi statutari o in adempimento a obblighi di legge, i dati potranno essere comunicati a soggetti terzi esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. Studio Commercialista, Istituto creditizio per riscossione quota associativa e altre competenze, Pubbliche Amministrazioni, Consulenti / collaboratori per corsi di formazione e altri progetti associativi, stampa e postalizzazione, ecc.).

✍ No Obbligo di INFORMATIVA in quanto trattandosi di persone giuridiche non rientrano nella definizione di interessati ex RGPD. Si valuta tuttavia opportuno, per trasparenza, completezza e chiarezza nella relazioni con gli Associati, fornire ugualmente informativa completa al momento dell'annovero.

✍ No CONSENSO in quanto trattandosi di persone giuridiche non rientrano nella definizione di interessati ex RGPD. Inoltre il trattamento è necessario per l'esecuzione degli obblighi e il raggiungimento dei fini stabiliti dallo Statuto e perché la comunicazione è funzionale all'esecuzione di tali attività. Si tratta di trattamento effettuato per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo e dallo statuto e con modalità di utilizzo rese note agli interessati all'atto dell'informativa che non pregiudicano i diritti e le libertà degli interessati.

 Dati di bilancio e dati relativi al business, assetto proprietario, eventuali dati di contatto (con relativo incarico aziendale) di personale dirigente o dipendente, posta elettronica e dati equivalenti sono necessari per l'adempimento delle finalità previste dallo Statuto Sociale e per lo svolgimento dell'ordinaria attività associativa (partecipazione alle attività di Organi statutari, Commissioni Tecniche, Gruppi di Lavoro, a convegni e altre iniziative associative riservate agli Associati, ecc.). Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per lo svolgimento dell'attività associativa, i dati potranno essere comunicati a soggetti terzi esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. stampa e postalizzazione, consulenti per lo sviluppo di progetti associativi).


✍ No Obbligo di INFORMATIVA in quanto trattandosi di persone giuridiche non rientrano nella definizione di interessati. Si valuta tuttavia opportuno, per trasparenza, completezza e chiarezza nella relazioni con gli Associati, fornire ugualmente informativa completa al momento dell'annovero.

✍ No CONSENSO in quanto trattandosi di persone giuridiche non rientrano nella definizione di interessati. Inoltre il trattamento riguarda principalmente dati relativi allo svolgimento di attività economica ed è necessario per l'esecuzione degli obblighi e il raggiungimento dei fini stabiliti dallo Statuto ed è funzionale all'esecuzione di tali attività. Si tratta di trattamento effettuato per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo e dallo statuto e con modalità di utilizzo rese note agli

interessati all'atto dell'informativa che non pregiudicano i diritti e le libertà degli interessati. Ciò vale anche per la comunicazione o diffusione, sempre del rispetto del complesso delle norme che regolano l'attività associativa ed in particolare del Codice Antitrust.


Nell'ambito delle specifiche finalità associative, tali dati possono pertanto essere comunicati e diffusi, anche fuori dall'ambito associativo, anche senza il consenso dell'interessato, purché nel rispetto della vigente normativa in materia di segreto aziendale e industriale, di tutela della concorrenza e del mercato e, con riferimento alle società emittenti di strumenti finanziari quotati, di abuso di informazioni privilegiate, comunicazioni illecite di informazioni privilegiate e manipolazione del mercato (cd Market Abuse Regulation).

Personale Dipendente degli Associati

 -Nome, Incarico aziendale, Posta elettronica aziendale e recapito telefonico sono necessari per lo svolgimento di attività associative previste dallo Statuto sociale (partecipazione a commissioni e/o gruppi di lavoro, altre iniziative e attività associative connesse ad approfondimenti sul mercato del factoring⁵). Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per il perseguimento delle finalità associative, lecite e prive del fine di lucro (es. diffusione per finalità di promozione e di conoscenza del settore in Italia e all'estero, corsi di formazione), i dati potranno essere comunicati a soggetti terzi esterni (es. pubblicazione della composizione delle commissioni sull'Annuario).


Tali dati possono essere forniti direttamente dall'interessato ma spesso sono forniti dagli Associati Assifact - datori di lavoro.

 **Obbligo di INFORMATIVA.**

 **No CONSENSO** perché il trattamento è necessario per l'esecuzione degli obblighi e il raggiungimento dei fini stabiliti dallo Statuto e perché la comunicazione è funzionale all'esecuzione di tali attività.

La raccolta, l'utilizzo e la comunicazione di tali dati rappresenta un interesse legittimo dell'Associazione in quanto il trattamento avviene nell'ambito del rapporto di associazione con l'Associato, rappresentato nelle Commissioni tecniche, nei GDL e negli organi statutari, dai propri dipendenti, per la realizzazione degli scopi statutari.

Si ritiene che tale interesse legittimo non possa generare rischi di particolare rilievo per i diritti e le libertà delle persone fisiche interessate.

 Nome, dati identificativi e anagrafici, con i relativi recapiti, dei soggetti membri del Consiglio di Assifact, del Comitato Esecutivo e del Collegio dei Revisori di Assifact sono necessari per l'adempimento degli obblighi amministrativi, contabili e fiscali. Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per l'esecuzione degli obblighi contrattuali o in adempimento a obblighi di legge, i dati potranno essere comunicati a soggetti terzi

⁵ As esempio, invio newsletter associativa, invio email alerting su principali contenuti e aggiornamenti del sito associativo, organizzazione workshop, pianificazione di iniziative di formazione e informazione su tematiche specifiche connesse al factoring.

esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. Studio Commercialista, Pubbliche Amministrazioni, ecc.).

✍ **Obbligo di INFORMATIVA**

✍ **No CONSENSO** perché i dati sono raccolti in base ad un obbligo di legge e il trattamento è necessario per l'esecuzione di obblighi derivanti dal rapporto associativo e perché la comunicazione è funzionale all'esecuzione di tale rapporto.

Fornitori, Consulenti, Collaboratori occasionali - Clienti

📁 Nome, Denominazione o Ragione Sociale, indirizzo e telefono e altri recapiti, altri dati identificativi (es. CF, P.IVA) e riferimenti bancari sono necessari per l'adempimento degli obblighi contabili e fiscali. Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per l'esecuzione degli obblighi contrattuali o in adempimento a obblighi di legge, i dati potranno essere comunicati a soggetti terzi esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. Studio Commercialista, Pubbliche Amministrazioni, ecc.).

✍ **Obbligo di INFORMATIVA**

✍ **No CONSENSO** perché i dati sono raccolti in base ad un obbligo di legge, il trattamento è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato e perché la comunicazione è funzionale all'esecuzione del contratto.

Terzi (utenti sito, soggetti che richiedono l'invio dell'e-mail alert "Factoring Outlook", della newsletter Fact&News, di materiale informativo, richiesta dati Credifact, altre richieste)

📁 Nome, indirizzo e telefono, posta elettronica sono necessari per l'esecuzione degli "obblighi contrattuali" ossia l'esecuzione di un "servizio" richiesto dall'interessato stesso. I dati sono forniti dall'interessato in via facoltativa, esplicita e volontaria. Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per l'esecuzione degli obblighi contrattuali, i dati potranno essere comunicati a soggetti terzi esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. Fornitore per stampa e postalizzazione).

✍ **INFORMATIVA:**

- **OBBLIGO** nell'ipotesi di predisposizione di moduli da compilare da parte di Assifact.
- **NO OBBLIGO** in caso di invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi e-mail associativi. Questo invio comporta la successiva acquisizione dell'indirizzo del mittente da parte di Assifact, necessario per rispondere alle richieste avanzate, unitamente agli eventuali altri dati personali inseriti nella comunicazione. La Privacy Policy è pubblicata e sempre disponibile sul sito associativo. Eventuale ulteriore informativa all'interessato sarà fornita dal titolare del trattamento solo nel caso di previsione di ulteriori trattamenti specifici con finalità diverse rispetto a quella connessa alla fornitura dei dati.

✍ No CONSENSO perché il trattamento è necessario per l'esecuzione di obblighi derivanti da un "contratto" (richiesta di servizio) del quale è parte l'interessato e perché la comunicazione è funzionale all'esecuzione di tale "contratto".

Terzi (rappresentanti e dipendenti di Banca d'Italia, altre istituzioni, ABI, Assilea, Assofin, altre associazioni e organizzazioni con cui Assifact ha stabili, regolari, consolidati contatti e collaborazioni)

📁 Nome, Ente o Istituzione, indirizzo e telefono, posta elettronica sono necessari per lo svolgimento delle finalità statutarie e di comune interesse con gli Enti e Istituzioni di riferimento degli interessati (ossia promuovere attività di studio e di ricerca riguardanti il factoring, favorire l'interlocuzione e il confronto su temi di interesse comune e collaborare con altri Enti, Associazioni, Istituzioni ed Organismi in genere nella soluzione dei problemi interessanti il factoring). Tipicamente questi dati sono forniti direttamente, esplicitamente e volontariamente dagli interessati e sono inseriti nell'archivio contatti dell'Associazione.

Questi dati sono trattati utilizzando strumenti manuali, informatici o altra modalità, anche non meccanizzata. Per l'esecuzione di suddette attività i dati potranno essere comunicati a soggetti terzi esterni che per conto dell'Associazione provvederanno all'espletamento di funzioni specialistiche specifiche (es. fornitore per stampa e postalizzazione, ecc.).

✍ NO obbligo di INFORMATIVA al momento del conferimento dei dati funzionali alla prosecuzione dei rapporti istituzionali. Eventuale ulteriore informativa all'interessato sarà fornita dal titolare del trattamento solo nel caso di previsione di ulteriori trattamenti specifici con finalità diverse rispetto a quella connessa alla fornitura dei dati.

✍ No Obbligo di CONSENSO

3.3 Misure di sicurezza e Controlli

Con riferimento a quanto sopra descritto, in relazione alla natura dei dati trattati, all'attività e ai trattamenti svolti da Assifact e alla sua struttura e dimensione organizzativa, si delineano di seguito le misure di sicurezza ritenute commisurate alla valutazione del rischio.

Ciascun incaricato riceve lettera di incarico con specifiche istruzioni per il trattamento e in cui risulta chiaro che l'incaricato può trattare i dati personali nel limite delle mansioni e per gli scopi che gli sono stati assegnati.

A ciascun incaricato è attribuito un codice identificativo personale necessario per accedere e utilizzare l'elaboratore. L'incaricato può autonomamente sostituire la propria parola-chiave d'accesso, purché ne dia notizia al soggetto preposto alla custodia.

In considerazione del fatto che vi sono più incaricati, viene individuato per iscritto un soggetto preposto alla custodia delle parole-chiave.

Lo stesso codice identificativo personale non può, neppure in tempi diversi, essere attribuito a diverse persone. In caso di annullamento dell'incarico, il codice deve essere disattivato. Il codice va disattivato anche dopo sei mesi di mancato utilizzo.

Il sistema informatico e la sua efficienza devono essere costantemente verificati, facendo ricorso ad un manutentore di sistema esterno, ed eventualmente approntate le modifiche relative al sistema hardware e software che si dovessero rendere necessarie data l'evoluzione tecnologica; ciò soprattutto al fine di proteggere gli elaboratori dal rischio di intrusione da parte di terzi non autorizzati.

Il manutentore del sistema verifica che i presidi tecnici-informatici, sulla base anche di un'analisi dei rischi, siano stati adottati e adeguati agli standard.

Assifcat, con la collaborazione del manutentore di sistema per le parti di sua competenza, deve predisporre un documento, che costituisce parte integrante del registro dei trattamenti, da cui risulta lo stato del sistema di sicurezza, con la descrizione dettagliata delle misure fisiche e logiche adottate.

Con riferimento al trattamento di dati con strumenti diversi da quelli elettronici o comunque automatizzati, gli atti e documenti in questione devono essere conservati in archivi a cui ha accesso il solo personale incaricato. Se si tratta di dati sensibili, i contenitori devono essere muniti di serratura.

Il titolare e il responsabile vigilano sul rispetto e sulla corretta applicazione della normativa privacy e della presente procedura, anche tramite controlli periodici.

L'adeguatezza della presente procedura viene valutata con cadenza semestrale.

Per quanto non indicato nella presente procedura, si fa rinvio a specifiche comunicazioni interne o destinate agli Associati, con particolare riferimento alle modalità di comunicazione di informazioni e materiali da e per gli Associati.