PRIVACY POLICY

Reg. UE 2016/679

Abaco s.p.a.

Head Office

Piazza Vilfredo Pareto 9
46100 Mantova

Versione 6

Revisione	Data pubblicazione	Autore	Motivo della revisione
0	22/05/2018	G.Ghilardi	Prima stesura
1	12/02/2020	G.Ghilardi	Revisione Organigramma
2	31/03/2021	G.Ghilardi	Introduzione protocollo 231. Ampliamento campo di applicazione sistemi di gestione integrati a servizi in modalità SaaS
3	16/11/2021	G.Ghilardi	Parti sottolineate Integrazione linee Guida ISO27017 e ISO27018
4	22/4/2022	G.Ghilardi	Specificata meglio integrazione branch UK ABACOGROUP Uk
5	24/05/2023	G.Ghilardi	Creata Policy Abaco UK LTD separata eliminati riferimenti in questa policy.
6	21/05/2024	G.Ghilardi	Inserita figura DPO

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento ha lo scopo di attestare la posizione di conformità di *Abaco .* rispetto agli obblighi introdotti dal **Regolamento Europeo 2016/679** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Le privacy policy di seguito indicate si applicano al trattamento di dati personali di terzi per i quali *Abaco .* risulta il Titolare del trattamento, così come definito dal Regolamento Europeo 2016/679.

La politica si applica a tutte le sedi Abaco Spa. Abaco UK LTD in quanto ente legale separato ha creato una Privacy Policy a se stante che segue la legge UK "UK GDPR". Al momento e fino a parere diverso il Regno Unito è equiparato ai paesi Europei da direttiva della comunità europea.

2. DEFINIZIONI

Ai fini del presente documento s'intende per:

1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e

soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

7) «**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;

8) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

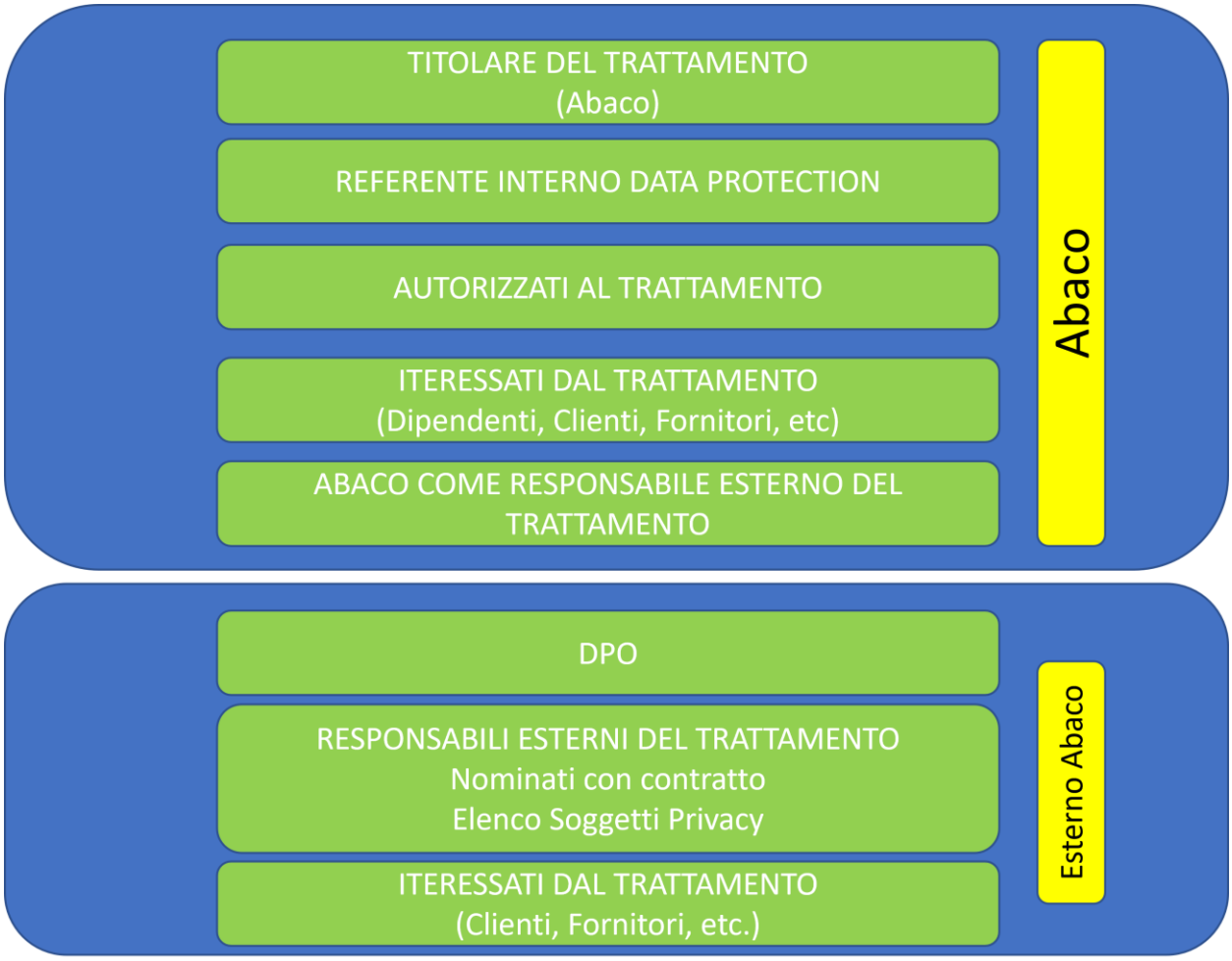
3. MODALITA' DEL TRATTAMENTO DEI DATI PERSONALI

Abaco tratta i dati personali di terzi osservando i seguenti principi:

a) trattati in modo lecito, corretto e trasparente nei confronti;
b) raccolti per finalità determinate, esplicite e legittime;
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

4. FIGURE COINVOLTE NEL TRATTAMENTO DEI DATI

4.1 Organigramma Privacy Aziendale



4.2 Soggetti interni ed esterni all'azienda

4.2.1 Titolare del trattamento

Abaco è il titolare del trattamento dei dati personali di persone fisiche così come definito dall'art. 4 comma 7 del REG (UE) 2016/679.
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento UE 2016/679.

4.2.2 Abaco Responsabile Esterno del trattamento

Abaco, ove necessario, può agire in qualità di Responsabile Esterno del trattamento di dati personali, ai sensi dell'art. 28 del REG (UE) 2016/679, nell'ambito di contratti di servizio stipulati con i propri clienti.

Abaco in qualità di Responsabile Esterno del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento UE 2016/679.

4.2.3 Responsabili Esterni del trattamento

Abaco ha individuato i "responsabili del trattamento" nelle figure esterne all'azienda che si occupano di:

- gestione di pratiche relative all'assunzione di lavoratori e alla gestione delle buste paga e/o altri servizi in materia di consulenza del lavoro;
- gestione di pratiche fiscali/contabili
- fornitori di servizi cloud e hosting
- fornitori di sistemi di gestione con assistenza
- fornitori di servizi di fornitura di SW in outsourcing o di prestazioni tipo "Time&Materiale"
- Fornitori di portali quali il portale per le segnalazioni Whistleblowing
- Aziende esterne del gruppo (Abaco UK LTD)

Con tali soggetti terzi Abaco sottoscrive un contratto di incarico per il trattamento dei dati ai sensi dell'art. 28 del REG (UE) 2016/679.

Secondo il contratto indicato i "responsabili del trattamento" individuati da Abaco hanno l'obbligo di:

- adottare misure tecniche e organizzative adeguate in modo tale che il trattamento dei dati personali di terzi, le cui categorie sono indicate nel contratto da Abaco, soddisfi i requisiti del regolamento UE 2016/679 e garantisca la tutela dei diritti degli interessati secondo quanto previsto dalla normativa vigente;
- garantire che le persone autorizzate al trattamento dei dati personali, le cui categorie sono indicate nel contratto da Abaco, si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure richieste ai sensi dell'articolo 32 REG (UE) 2016/679;
- tenendo conto della natura del trattamento, assistere ABACO con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del REG. UE 2016/679;
- assistere ABACO nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del REG(UE) 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su richiesta del titolare del trattamento, cancellare o restituire tutti i dati personali, le cui categorie sono sopra indicate, dopo che è terminata la prestazione dei servizi relativi al trattamento. In entrambi i casi il Responsabile provvederà a rilasciare al Titolare, dietro sua richiesta, apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni degli interessati;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Reg. UE 2016/679;

- comunicare tempestivamente al Titolare istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di Controllo e dalle Autorità Giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali;
- selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di cui alla normativa applicabile e garantisca la tutela dei diritti degli interessati;
- stipulare specifici contratti, o altri atti giuridici, con i sub-responsabili a mezzo dei quali il Responsabile descriva analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Titolare sul Responsabile ai sensi della normativa vigente (art. 28 comma 4 REG UE 2016/679);
- conservare nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili coinvolti, così come previsto dalla normativa vigente (art. 28 comma 4 REG UE 2016/679).

Con la stipula dei contratti di incarico per il trattamento dei dati ai sensi dell'art. 28 del REG (UE) 2016/679, ABACO conferisce autorizzazione scritta generale ai Responsabili del trattamento a poter ricorrere a eventuali ulteriori responsabili del trattamento ("sub-responsabile/i") stabiliti all'interno dell'Unione Europea.

4.2.4 Ufficio Compliance

Al fine di adempiere agli obblighi previsti dal Reg. UE 2016/679 Abaco ha individuato nella funzione aziendale dell'"Ufficio Compliance" il riferimento interno all'azienda per l'attuazione delle prescrizioni introdotte dalla normativa Europea per tutte le sedi di Abaco.
Di seguito vengono riportati in sintesi i principali compiti e mansioni dell'ufficio compliance in materia di trattamento dei dati personali di persone fisiche e libera circolazione dei dati.

Compiti e mansioni:

- Individuazione dei "responsabili del trattamento";
- Predisposizione dei contratti di incarico per il trattamento dei dati ai sensi dell'art. 28 del REG (UE) 2016/679 con i responsabili del trattamento;
- Archiviazione dei contratti con i responsabili del trattamento in essere e gestione delle relative modifiche;
- Predisposizione ed aggiornamento del Registro dei trattamenti;
- Predisposizione delle informative agli interessati al trattamento;
- Gestione delle attività da intraprendere per l'esercizio dei diritti degli interessati;
- Gestione delle attività da intraprendere per la notifica delle violazioni di dati personali;
- Pianificazione e organizzazione della formazione del personale in materia di privacy;
- Responsabile del sistema di gestione aziendale ISO 27001 integrato con le linee guida ISO27017 e ISO27018, a cui si rimanda per l'applicazione delle misure tecnico/organizzative per il trattamento in sicurezza dei dati personali.

4.2.5 Autorizzati al trattamento

Nel Reg. UE 2016/679 non è esplicitamente richiamata la figura dell'"incaricato del trattamento", prevista invece dalla precedente normativa d.lgs. 196/2003 "Codice privacy".

Abaco revede di usare la nomenclatura "Autorizzati al trattamento" per identificare quei soggetti, diversi dai responsabili del trattamento, che lavorano per conto dell'azienda in tutte le sedi e che possono trattare in funzione del ruolo aziendale ricoperto dati personali di terzi.
Per autorizzati al trattamento si intendono pertanto:

- dipendenti o collaboratori aziendali;

Si precisa che tali soggetti possono ricoprire anche il ruolo di "interessati al trattamento".
Tuttavia, nel ruolo di "autorizzati al trattamento" hanno l'obbligo di:

- trattare in modo lecito e secondo correttezza i dati personali delle persone fisiche;
- trattare i dati personali delle persone fisiche per gli scopi determinati, funzionali, espliciti e legittimi in base al ruolo aziendale ricoperto e alle relative mansioni lavorative;
- attivarsi per far si che i dati trattati siano esatti e per quanto possibile aggiornati;
- usare all'interno come all'esterno dell'azienda la massima discrezione sui dati personali di cui si ha conoscenza, curando attentamente la loro protezione, in particolare nei casi in cui
  le informazioni riguardino elementi caratteristici quali lo stato di salute, di famiglia o aspetti relativi all'identità economica, culturale o sociale;
- non diffondere all'esterno dell'azienda dati personali di persone fisiche, salvo i casi in cui ciò sia necessario per lo svolgimento degli incarichi affidati;
- utilizzare esclusivamente gli strumenti ed i programmi forniti o autorizzati dall'azienda e soltanto per svolgere le mansioni assegnate;
- conoscere il contenuto del presente documento (Manuale Privacy);
- applicare per quanto di competenza le procedure previste dal Sistema di Gestione della Sicurezza delle Informazioni – certificato ISO 27001.

Abaco ha provveduto a nominare, con nomina della direzione (6.17 MOD AUT Autorizzazione Interna Trattamento Dati), gli autorizzati per il trattamento dei dati di Abaco e dei propri dipendenti/collaboratori di tutte le sedi e branch e si impegna a nominare gli autorizzati al trattamento dei dati in base alle mansioni ricoperte e al trattamento previsto di dati personali sin dalla assunzione.

4.2.6 Interessati al trattamento

L'interessato è:

- la persona fisica (identificata o identificabile) a cui il dato personale si riferisce.

Le categorie di interessati di cui Abaco tratta i dati personali sono riportati nel registro dei trattamenti la cui gestione è di seguito descritta.
L'esercizio dei diritti degli interessati viene garantito da Abaco . con le modalità riportate nel presente documento.

4.3 Figure non obbligatorie

4.3.1 DPO (Data Protection Officer – Responsabile della protezione dei dati)

In base a quanto previsto dall'art. 37 del REG (UE) 2016/679, il Titolare del trattamento deve designare un DPO nel caso in cui:

- il trattamento venga effettuato da un'autorità pubblica o da un organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);

- qualora le attività principali del Titolare e del Responsabile/i del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- nell'ipotesi in cui le attività principali di suddetti soggetti consistano in trattamenti su larga scala di categorie particolari di dati personali (dati sensibili, dati genetici, biometrici, dati giudiziari).

ABACO non rientra nelle casistiche sopra indicate per le quali la figura del DPO risulta obbligatoria, ma nonostante non abbia l'obbligo, per avere un maggiore controllo e una entità terza esterna che possa fare da collettore delle problematiche inerenti al trattamento dei dati, ha deciso di nominare DPO l'azienda Seprim Srl nella persona di Andrea Parma, cono notifica ufficiale al garante della privacy. Il DPO può essere contattato all'indirizzo dpo-mantova@abacogroup.eu . Il DPO conduce annualmente un audit di revisione dei processi e dei documenti.

4.3.2 Rappresentante UE

Abaco non è tenuta alla nomina di un Rappresentante UE in quanto l'azienda ha sede all'interno dell'Unione Europea.

4.3.3 Legislatura di riferimento della ABACO UK LTD

Abaco considera ABACO UK LTD equiparata alle sedi Italiane in materia di protezione dei dati personali. Questo anche alla luce della decisione della Comunità Europea del 28/6/2021 che a seguito della Brexit emana il provvedimento di adeguatezza con data di termine nel 2025. E' ritenuta di livello appropriato la protezione e la legislazione inglese (General Data Protection Regulation (UK GDPR)).

5. REGISTRO DEI TRATTAMENTI

Allo scopo di disporre di un quadro aggiornato dei trattamenti effettuati Abaco . si è dotata del registro dei trattamenti di cui all'art. 30 del Reg. UE 2016/679.
L'ufficio compliance provvede a redigere tale registro e a mantenerne il contenuto costantemente aggiornato per tutte le sedi Abaco.
Il registro contiene:

- Dati relativi al titolare del trattamento
- Categorie degli interessati
- Categoria dei dati personali trattati
- Dettaglio dei dati personali trattati in relazione alla categoria di appartenenza
- Modalità di raccolta dei dati personali
- Termine per la cancellazione dei dati personali
- Finalità del trattamento
- Destinatari a cui vengono comunicati i dati personali (interni/esterni all'azienda)
- Trasferimento di dati personali a paesi terzi/organizzazioni internazionali
- Strumenti coinvolti nel trattamento
- Misure di sicurezza tecniche/organizzative

6. INFORMATIVE AGLI INTERESSATI E CONSENSO AL TRATTAMENTO

Il modello di informativa predisposto da Abaco e rivolto agli interessati del trattamento contiene:

a) l'identità e i dati di contatto del titolare del trattamento;
b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) le eventuali categorie di destinatari dei dati personali;
d) l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
e) periodo di conservazione dei dati personali;
f) i diritti dell'interessato;
g) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati.

L'ufficio compliance provvede a personalizzare le informative in funzione della categoria di interessati a cui è rivolta.
In relazione alla navigazione Internet ed all'utilizzo dei Cookies durante la navigazione stessa sui siti internet aziendali l'informativa e i consensi sono stati affidati a fornitore esterno specializzato (Iubenda) che fornice la compliance alle ultime linee guida del Garante.
Il controllo delle informative per le piattaforme web-based sviluppate da Abaco è gestita dal reparto Compliance in collaborazione con il gruppo di sviluppo.
Il dettaglio sulle modalità di gestione di tutti i trattamenti Privacy è contenuto nelle istruzioni operative IST 07.02.01 e IST 07.02.02.
Di seguito riportiamo le principali modalità di trasmissione delle informative ai soggetti che interagiscono con Abaco.

6.1 Modalità di trasmissione delle informative agli interessati

a) Dipendenti aziendali e/o collaboratori
L'ufficio compliance provvede a tenere aggiornate le informative per i dipendenti e i collaboratori in base all'evolversi del contesto e delle normative applicabili.
E' demandato all'ufficio HR la consegna e l'archiviazione delle informative firmate dai dipendenti in fase di assunzione sul sistema integrato aziendale, insieme a tutto il pacchetto di documentazione previsto in ingresso in azienda. Inoltre, nei corsi iniziali viene inserita anche una formazione sulla privacy.
In caso di integrazione della informativa standard è l'ufficio compliance che si occupa di integrare i testi e provvedere ad ottenere l'integrazione del consenso da parte di tutti i soggetti interessati.
Nel caso di trattamento di dati personali di familiari maggiorenni a carico viene richiesto il consenso esplicito dell'interessato mediante firma sull'informativa.

b) Clienti/Fornitori (persone fisiche)

Le comunicazioni di Abaco Spa con i propri clienti/fornitori che avvengono via mail contengono, come, tutti gli indirizzi mail di *Abaco,* un link che rimanda al sito Abacogroup dove è pubblicata nel footer di ogni pagina l'informativa privacy ai sensi dell'art. 13 del Reg. Ue 2016/679.

Per quanto riguarda i contatti che potenziali clienti possono chiedere attraverso il sito internet aziendale, il form per la richiesta contiene il link alla informativa e richiede il consenso esplicito, obbligatorio per il normale trattamento dei dati forniti per la richiesta di informazioni, mentre è facoltativo per l'inserimento in campagne marketing.

E' l'ufficio Marketing che si occupa di controllare i consensi in base alle comunicazioni che intende effettuare.

Per quanto riguarda gli eventi, anche online come ad esempio i webinair, è stata prevista una informativa specifica, anch'essa viene predisposta dall'ufficio Compliance e poi inviata e trattata dall'ufficio Marketing.

Le regolamentazioni contrattuali con i clienti e i fornitori riguardo agli adempimenti di ciascun soggetto sul trattamento dei dati sono esplicitate nel contratto e in eventuali allegati specifici.

Anche riguardo a questo punto si rimanda all'istruzione operativa citata in precedenza.

c) Persone fisiche che si registrano sui portali aziendali

I portali aziendali, che prevedono la raccolta di dati personali di persone fisiche, riportano pubblicata l'informativa privacy ai sensi dell'art. 13 del Reg. UE 2016/679.

A seguito della presa visione dell'informativa pubblicata, l'interessato, prima della trasmissione dei suoi dati, deve fornire il proprio consenso esplicito (doppio) al trattamento mediante flag sull'icona corrispondente.

Una volta dato il consenso il sistema invia una mail all'indirizzo privacy@abacogroup.eu con i dati inseriti dell'interessato.

L'ufficio compliance provvede ad archiviare le mail ricevute.

Lo stesso avviene per i servizi forniti in modalità Saas e per le applicazioni pubblicate sugli store per i dispositivi mobile. Anche riguardo a questo punto si rimanda alle istruzioni operative IST 07.01 e IST 07.02.02

d) Informativa Cookies

Il sito internet aziendale presenta una informativa cookies che rispecchia le indicazioni del Garante, riportando in modo completo tutti i cookie utilizzati dal sito, suddivisi in tecnici e di terze parti, e dando all'utente la possibilità di accettare o disabilitare tali cookies al primo accesso al sito o anche successivamente.

Lo stesso metodo è utilizzato anche sul sito internet relativo al portale Abaco Farmer e all'interno delle applicazioni sviluppate da Abaco.

Al momento per facilitare il compito dell'ufficio compliance e del reparto Comunicazione che manutiene il sito corporate e di Abaco Farmer la gestione della informativa cookies è stata affidata ad un fornitore esterno (Iubenda) che garantisce la compliance alle direttive del Garante.

E' cura dell'ufficio compliance controllare che le informative siano aggiornate, aggiornare le pubblicazioni sulle applicazioni sviluppate da Abaco.

7. ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

I diritti degli interessati previsti dal Reg. UE 2016/679 sono i seguenti:

Art. 15 Reg. UE 2016/679
Diritto di accesso

1.L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2.Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3.Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4.Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Art. 16 Reg. UE 2016/679
Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art. 17 Reg. UE 2016/679
Diritto alla cancellazione (diritto all'oblio)

1.L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2.Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3.I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 18 Reg. UE 2016/679
Diritto di limitazione di trattamento

1.L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2.Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3.L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Art. 19 Reg. UE 2016/679
Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 20 Reg. UE 2016/679
Diritto alla portabilità dei dati

1.L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);
b) il trattamento sia effettuato con mezzi automatizzati.

2.Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3.L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4.Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Art. 21 Reg. UE 2016/679
Diritto di opposizione

1.L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2.Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3.Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4.Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5.Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6.Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art. 22 Reg. UE 2016/679
Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1.L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2.Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.

3.Nei casi di cui al paragrafo *2*, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4.Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Premesso che *Abaco .* non fa attività di profilazione, l'esercizio dei diritti degli interessati viene garantito con le seguenti modalità:

- L'interessato è informato che può esercitare i suoi diritti mediante richiesta a privacy@abacogroup.eu. Tale informazione è presente nelle "informative sul trattamento dei dati personali" che *Abaco .* invia a tutti gli interessati.
- L'ufficio compliance, che legge l'indirizzo di posta elettronica privacy@abacogroup.eu, prende in carico la richiesta di esercizio dei diritti dell'interessato e provvede a:
  a) inserire la tipologia di richiesta nel "registro richieste diritti privacy", indicando data di ricezione, generalità dell'interessato, tipologia di richiesta, uffici interni di competenze e/o destinatari esterni coinvolti;
  b) attivarsi per coordinare le attività interne propedeutiche al soddisfacimento della richiesta dell'interessato;
  c) verificare che la richiesta dell'interessato sia stata correttamente presa in carico da tutti gli uffici interni di competenza e/o destinatari esterni coinvolti;
  d) comunicare all'interessato che *Abaco .* ha provveduto ad attivarsi per garantire l'esercizio del diritto dell'interessato, adempiendo alla richiesta pervenuta.

8. MISURE DI SICUREZZA TECNICO/ORGANIZZATIVE

Le misure di sicurezza tecnico/organizzative, implementate da *Abaco*, garantiscono un livello di sicurezza adeguato nel trattamento dei dati personali di persone fisiche.
Tali misure garantiscono in linea generale:

a) la pseudonimizzazione e la cifratura dei dati personali, ove possibile;
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) la possibilità di testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Abaco è in possesso della certificazione ISO 27001 (sistema di gestione della sicurezza delle informazioni) estesa alle linee guida ISO27017 e ISO27018.
Le procedure per le tecniche di sicurezza delle informazioni si applicano anche al trattamento dei dati personali di persone fisiche.

Pertanto, per la definizione specifica e l'applicazione delle misure tecnico/organizzative in materia di privacy si rimanda al Sistema di Gestione della Sicurezza delle Informazioni implementato da *Abaco.*

8.1 Cancellazione dei dati personali dagli archivi

La cancellazione dei dati personali degli archivi di *Abaco* nei casi in cui siano superati i termini di legge e/o quelli previsti all'interno del "registro dei trattamenti", viene effettuata con le seguenti modalità:

a) *Archivi cartacei*: una volta all'anno ufficio compliance, in collaborazione con uffici competenti, contrassegna la documentazione cartacea che ha superato il limite di conservazione stabilito ed incarica una ditta terza per il macero.

b) *Posta elettronica*: gli incaricati al trattamento devono provvedere a cancellare dai propri indirizzi di posta le mail che abbiano superato il limite di conservazione stabilito, seguendo le modalità del browser di posta elettronica impiegato. L'ufficio compliance verifica a spot che tale cancellazione sia stata effettuata.

c) *Archivi informatici*: gli incaricati al trattamento devono provvedere a cancellare dai propri archivi informatici i documenti contenenti dati personali di persone fisiche che abbiano superato il limite di conservazione stabilito. L'ufficio compliance verifica a spot che tale cancellazione sia stata effettuata.
Per tutti i documenti presenti in azienda, una volta ritenuti non più utili, essi vengono eliminati manualmente e smaltiti come previsto dalla politica ambientale anche attraverso l'uso di macchinari distruggi documento.

9. NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI

Premesso che in funzione dei dati personali di persone fisiche trattati, in caso di violazione, difficilmente si possa configurare una delle seguenti ipotesi:

- danni fisici
- discriminazione
- furto o usurpazione di identità
- perdite finanziarie
- pregiudizio alla reputazione
- danno economico
- danno sociale
- perdita di riservatezza di dati protetti da segreto professionale

L'ufficio compliance provvederà ad analizzare la violazione avvenuta e verificare se essa rappresenti un rischio per i diritti e le libertà delle persone fisiche interessate.
Se dalla violazione si possa configurare una delle ipotesi sopra indicate, il Titolare del trattamento provvederà alla notifica all'autorità di controllo competente (vedi procedura per la notifica delle violazioni di dati personali, punto 9.2), per tutte le sedi Abaco.

In caso contrario la violazione subita verrà comunque documentata secondo le modalità di seguito indicate (vedi gestione delle violazioni di dati personali, punto 9.1) ma non notificata all'autorità competente.

9.1 Gestione delle violazioni di dati personali

In caso di violazione l'ufficio compliance provvede alla compilazione del modulo "registro reclami clienti, non conformità interne e violazioni di dati personali", documentando:

- la data di riscontro della violazione
- da chi è stata rilevata la violazione
- la descrizione della violazione
- il livello di gravità della violazione (lieve – non necessaria notifica Garante privacy/ grave – necessaria notifica Garante privacy)
- analisi delle cause che hanno portato alla violazione
- soluzione adottata
- stato, esito, data di attuazione della soluzione adottata
- eventuale azione correttiva che si ritiene necessaria per il non ripetersi dello stesso tipo di violazione subita
- tempi di attuazione, incaricato, chiusura dell'azione correttiva

9.2 Procedura per la notifica delle violazioni

Autorità di riferimento: Garante privacy
Il Titolare del trattamento, nei casi indicati al punto 9 del presente documento, procede alla notifica delle violazioni così come indicato dal Regolamento UE 2016/679 entro 72 ore dall'accadimento.
L'ufficio compliance provvede ad applicare la procedura definita attualmente dal Garante Privacy per la notifica delle violazioni, pertanto:

1) Entro 24 ore dalla violazione fornisce al Garante Privacy sommarie informazioni in relazione alla violazione verificatasi, integrando poi la comunicazione in un momento successivo. Tali sommarie informazioni devono consentire all'Autorità di effettuare una prima valutazione dell'entità della violazione e comprendono pertanto:

- i dati identificativi del titolare del trattamento;
- una breve descrizione della violazione;
- l'indicazione della data anche presunta della violazione e del momento della sua scoperta;
- l'indicazione del luogo in cui è avvenuta la violazione dei dati;
- l'indicazione della natura e del contenuto dei dati anche solo presumibilmente coinvolti;
- una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Per la comunicazione verrà utilizzato il format attualmente predisposto dall'Autorità "modello di segnalazione data breach" disponibile sul sito internet del Garante privacy.

2) Entro 72 ore dalla violazione l'ufficio compliance provvederà a comunicare al Garante le modalità con le quali si è posto rimedio alla violazione e le misure adottate o che si prevedono di adottare per prevenire ulteriori violazioni della medesima specie;

3) Entro 72 ore dalla violazione l'ufficio compliance provvederà a comunicare all'interessato:
- la natura della violazione
- la tipologia di dati personali coinvolti
- le raccomandazioni che eventualmente l'interessato dovrebbe attuare per attenuare i possibili effetti negativi
- le misure adottate o che si prevedono di adottare a cura del Titolare del trattamento per prevenire ulteriori violazioni

10. FORMAZIONE ED INFORMAZIONE DEL PERSONALE

10.1 Formazione

La formazione del personale aziendale in materia di privacy ed in particolare sulla revisione delle procedure interne per il recepimento del Reg. UE 2016/679 avviene seguendo le procedure aziendali del sistema di gestione ISO 9001:2015 in materia di formazione interna.

10.2 Informazione

Tutti gli incaricati aziendali del trattamento hanno a disposizione il presente documento, caricato sui canali interni e sul sito aziendale, al quale si devono attenere per la gestione dei dati personali di terzi.
Inoltre, agli incaricati del trattamento, ricoprendo anche il ruolo di interessati al trattamento, viene, come indicato al punto 6, trasmesso il training sulla privacy che sintetizza la posizione aziendale rispetto al nuovo Regolamento Europeo ed illustra i diritti degli interessati.
A tutti i nuovi assunti viene fatto un corso iniziale sul nuovo regolamento e sulle procedure interni in materia di protezione dei dati differenziato a seconda del ruolo ricoperto.

11. DOCUMENTI CORRELATI

- modelli di informativa al trattamento dei dati
- modello del contratto di incarico per i responsabili del trattamento
- registro trattamenti
- registro richieste diritti privacy
- registro reclami clienti, non conformità interne e violazioni di dati personali
- organigramma aziendale
- 6.17 MOD AUT Autorizzazione Interna Trattamento Dati