

Euro Informatica Sistemi S.r.l.

SEDE

Via Principe di Napoli, 126
00062 Bracciano (Roma)
Tel. 06.99.80.31.31 – Fax 06.99.80.3027

FILIALE

Via Fiume 55/a/b
00055 Ladispoli (Roma)
Tel. 06.99.22.2012 – Fax 06.99.22.6763

www.euroinf.it

info@euroinf.it

info@pec.euroinf.it

GDPR AUDIT CHECK LIST GENERALE (VERS. 1.10 DEL 12/5/2018)

CONSULENTE: _____ DATA VISITA: _____
RAGIONE SOCIALE OPPURE NOME E COGNOME _____
INDIRIZZO SEDE LEGALE CAP CITTA' PROVINCIA _____
TELEFONO FAX PARTITA IVA _____
E-MAIL E/O WEB SITE REFERENTE _____
ATTIVITA' PRINCIPALE (descrivere l'attività) _____
ALTRE ATTIVITA' _____
ALTRE SEDI AZIENDALI (ITALIA) _____
ALTRE SEDI AZIENDALI (PAESI UE) _____
ALTRE SEDI AZIENDALI (PAESI EXTRA UE) _____

1. L'azienda svolge una funzione di pubblico interesse? SI NO

Es. Gestione di depuratori, trasporti, servizi idrici, gestione edilizia popolare, etc.

2. Tipologia dei dati personali oggetto di trattamento

(SELEZIONARE SOLO SE NON RIGUARDANO IL PERSONALE DIPENDENTE)

- Dati personali identificativi (anche ad. Es. cookies – indirizzi IP)
- Dati personali idonei a rivelare l'origine razziale ed etnica
- Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere
- Dati personali idonei a rivelare le opinioni politiche
- Dati personali idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazione a carattere religioso, filosofico, politico o sindacale
- Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- Dati giudiziari

3. Informativa ed altri adempimenti

Si utilizzano moduli per l'informativa sul trattamento dei dati SI NO

Clienti Fornitori Dipendenti

· Acquisire copia informative

Tra i clienti ci sono minori? SI NO

Il dato viene usato solo per lo scopo per il quale è stato raccolto?

SI NO Altri scopi (specificare) _____

4. Consenso

Si utilizzano moduli per l'acquisizione del consenso sul trattamento dei dati SI NO

· Acquisire moduli consenso

5. Comunicazioni Commerciali

L'azienda svolge azioni di comunicazioni commerciali nei confronti dei clienti (telefono, SMS, mail marketing)?

SI NO

Se SI come viene svolta l'attività? Internamente Esternalizzata

Con quale modalità? Telefono Call center interno Telefonate dirette

(n.b. se l'azienda è dotata di call center interno compilare punto 8 Check list)

SMS Mail marketing Altro _____

L'azienda ha fornito adeguata informativa ed acquisito il consenso dei propri clienti all'invio di comunicazioni commerciali?

SI NO

· Acquisire copia informativa e modulo di consenso

Nel caso di attività di mail marketing o SMS indicare la piattaforma utilizzata.

SUGGERIMENTO: Il fornitore di piattaforme di mail marketing o SMS deve consentire una corretta gestione del servizio quale: possibilità per gli utenti di cancellarsi dalla lista o modificare alcuni dati in modo facile e immediato, inserire come mittente delle comunicazioni un indirizzo fisico reale.

6. Sito Web

L'azienda ha un sito web? SI NO

Se SI indicare l'indirizzo del sito web _____

L'azienda ha un portale di e-commerce? SI NO

Se SI indicare l'indirizzo del sito e-commerce _____

Che protocolli di protezione utilizza per il sito web/e-commerce?

SSL/HTTPS ALTRO _____

L'azienda acquisisce dati personali dal sito web/e-commerce per mezzo di form di richiesta info?

SI NO

Se SI è stata predisposta l'informativa per il form e richiesto il consenso?

SI NO

Come viene gestito il sito web? Internamente In esterno

Se la gestione è esternalizzata indicare il nome della società esterna e i servizi gestiti?

Nome società _____

Servizi: Seo Hosting e mail Altro _____

Nome società _____

Servizi: Seo Hosting e mail Altro _____

Nome società _____

Servizi: Seo Hosting e mail Altro _____

Le società esterne gestori del sito visualizzano i dati acquisiti dal form? SI NO

Se SI indicare il nome della società _____

Le società esterne gestori del sito accedono al Data Base del sito? SI NO

Se SI indicare il nome della società _____

Le società esterne gestori del sito accedono all'FTP del sito? SI NO

Se SI indicare il nome della società _____

Dove risiede il sito web? Server interno Server esterno

Se Server esterno da quale società è fornito? (indicare il nome) _____

Dove fisicamente risiede il server? Italia UE Extra UE

L'azienda cede i dati acquisiti dal sito a terzi? SI NO

Se SI indicare il nome della società terza e le modalità di cessione.

SUGGERIMENTO

I. La **privacy policy** del sito deve essere fornita dalla società che ha realizzato il sito web. Nel caso il sito ne sia sprovvisto non è possibile implementarla senza avere gli accessi al sito in qualità di amministratore. E' possibile acquistare da terzi il servizio di gestione del sito e della privacy policy come **SERVIZIO AGGIUNTIVO**.

II. La società fornitrice del **servizio di hosting** nel contratto deve indicare clausole di garanzia di servizio conformi al GDPR, nonché consentire di modificare utente e password fornite in sede di acquisto dello spazio hosting

III. La società fornitrice del **servizio di posta elettronica** deve consentire il cambio password in sede di creazione delle caselle. Il fornitore del servizio deve garantire, così come previsto dal GDPR, in caso di cambio provider la possibilità di ricevere in un file la copia di tutta la posta e della rubrica.

6.1 Sito Web – Cookie

L'azienda utilizza cookies sul proprio sito web? SI NO

Se SI indicare il tipo di cookie: Tecnico Profilazione

SUGGERIMENTO: I **cookie tecnici** sono quelli necessari alla normale fruizione e navigazione del sito, i **cookie di profilazione** creano profili relativi all'utente e vengono utilizzati per inviare messaggi pubblicitari in linea con le preferenze manifestate durante la navigazione in rete.

Nel caso in cui il sito sia sprovvisto della **gestione dei cookie** (informativa, privacy policy, e gestione del consenso se necessario) è possibile acquistare da terzi il servizio di gestione dei cookie come **SERVIZIO AGGIUNTIVO**.

7. Attività Social

L'azienda acquisisce dati tramite le pagine social aziendali mediante form di acquisizione dati?

SI NO

Se SI specificare il tipo di dato acquisito

nome utente, acronimo residenza età indirizzo mail numero di telefono

altro (specificare) _____

Utilizzo del dato (al di fuori delle pagine social) nessun utilizzo

promuovere attività aziendale invito a workshop/eventi altro (specificare) _____

L'azienda cede i dati acquisiti a terzi? SI NO

Se SI indicare il nome della società terza e le modalità di cessione.

SUGGERIMENTO: I **dati acquisiti dalle pagine social aziendali** devono gestiti dalla società che amministra le pagine social. Il dato non può essere utilizzato fino a che non viene fornita l'informativa agli utenti e questi non abbiano prestato il loro consenso.

Nel caso il form di acquisizione dati sia sprovvisto dell'informativa e del consenso non è possibile implementarlo senza avere gli accessi alle pagine social in qualità di amministratore.

E' possibile acquistare da società terzi il servizio di gestione dei social come **SERVIZIO AGGIUNTIVO**.

8. Call center

DA COMPILARE SE NEL PUNTO 5 E' STATO SELEZIONATO IL CALL CENTER

L'azienda utilizza liste già consensiate? SI NO

L'azienda provvede al ripulire le liste per mezzo del registro delle opposizioni? SI NO

L'azienda ha dato istruzioni ai propri operatori di annotare la revoca del consenso? SI NO

L'azienda utilizza le numerazioni come dalle nuove disposizioni legislative sul Telemarketing? SI NO

- *n.b. Compilare il punto 10 indicando gli addetti al call center*

9. Particolari tipi di trattamento

L'azienda non effettua nessun tipo di trattamento come segue

Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".

Esempi:

istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio

un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo

una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute

una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web

Decisioni automatizzate che producono significativi effetti giuridici o di analogo natura: trattamenti finalizzati ad assumere decisioni su interessati che producano "effetti giuridici sulla persona fisica" ovvero che "incidono in modo analogo significativamente su dette persone fisiche"

Esempio: quando il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione

Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico"

Dati sensibili o dati di natura estremamente personale: per esempio, informazioni sulle opinioni politiche di una persona fisica oltre ai dati personali relativi a condanne penali o reati.

Esempio:

Ospedale che conserva le cartelle cliniche dei pazienti,

Investigatore privato che conserva informazioni su soggetti responsabili di reati.

Dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza)

Dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione

Dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti.

Dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.

Trattamenti di dati su larga scala:

I fattori al fine di stabilire se un trattamento sia svolto su larga scala:

a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;

b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;

c. durata, o persistenza, dell'attività di trattamento;

d. ambito geografico dell'attività di trattamento.

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

Dati relativi a interessati vulnerabili.

Esempio

Minori

Dipendenti,

Soggetti con patologie psichiatriche,

Richiedenti asilo,

Anziani,

Pazienti.

Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative,

Esempio

Associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici.

Una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone.

Tutti quei trattamenti che, di per sé, "impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Esempio

Trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto.

Screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

Se il cliente effettua almeno due tipi dei trattamenti sopra indicati, descrivere il trattamento complessivo e compilare l'allegato DPIA.

10. Soggetti che effettuano il trattamento dei dati

Indicare numero complessivo dipendenti: _____

Titolare del trattamento: _____

Responsabile del trattamento: _____

Sub responsabili del trattamento: _____

NEL CASO DI STUDI DI PROFESSIONISTI elencare gli eventuali tirocinanti/collaboratori e i relativi trattamenti

Collaboratori (elenco) Trattamenti effettuati

Nome _____ Clienti Fornitori Collaboratori

Lo Studio si avvale della consulenza di altri PROFESSIONISTI?

SI NO

Indicare nominativo: _____

Addetti al reparto amministrativo e gestione del personale

Indicare numero: _____

Nome _____ Amministrazione Gestione Personale

Addetti al reparto commerciale

Indicare numero: _____

Nome _____ Acquisti Vendite

Nome _____ Acquisti Vendite

Nome _____ Acquisti Vendite

Nome _____ Acquisti Vendite

Altri reparti che effettuano il trattamento dei dati

Reparto: _____ Numero addetti: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Reparto: _____ Numero addetti: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Reparto: _____ Numero addetti: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Nome: _____ Reparto: _____

Elencare il rappresentante legale/amministratore, i soci e gli eventuali trattamenti

Rappresentante Legale/Amministratore: _____

Soci (elenco) Effettuano trattamenti

_____ SI NO

Se SI selezionare : Amministrazione Gestione personale Acquisti Vendite

_____ SI NO

Se SI selezionare : Amministrazione Gestione personale Acquisti Vendite

_____ SI NO

Se SI selezionare : Amministrazione Gestione personale Acquisti Vendite

Amministratore di sistema: SI NO

Se [SI] (indicare nominativo) _____

Nel caso in cui l'azienda **non dispone** di un amministratore di sistema, ha al suo interno un **addetto** che si occupa della rete aziendale? Se Si (indicare nominativo): _____

Gli addetti al trattamento hanno ricevuto apposita formazione sul trattamento dati:

SI NO

In che modalità: formazione in aula video corsi online

altro (specificare) _____

SUGGERIMENTO: Se il personale non ha mai stato formato sul trattamento dati è consigliabile suggerire al cliente la formazione del proprio personale

DPO – DATA PROTECTION OFFICER

L'Azienda svolge trattamenti per cui il DPO è obbligatorio? SI NO

(se SI barrare il trattamento interessato)

monitoraggio continuativo e su larga scala di persone fisiche

trattamento di dati sensibili o giudiziari su larga scala

Responsabili esterni (indicare nominativi)

Vengono ceduti dati personali a terzi SI NO

Consulente del lavoro _____ Commercialista _____

Avvocato _____ Gestore pagine social _____

- Gestore sito web _____ Fornitore di servizi di cloud server _____
- Altri fornitori di servizi cloud (specificare) _____
- Fornitore assistenza sul software gestionale _____
- assistenza il loco assistenza da remoto
- Attività di call center _____
- Agenti e rappresentanti di commercio

- Società di recupero credito _____
- Gestore impianto videosorveglianza _____
- Assistenza Tecnica _____
- Altro (descrivere) _____

11. Descrizione della sede dell'azienda

- Stabilimento industriale**
- Dislocazione ufficio amministrativo
- Piano (es.piano terra, primo piano) _____
- N. stanze _____
- Dislocazione ufficio commerciale
- Piano (es.piano terra, primo piano) _____
- N. stanze _____
- Dislocazione altri uffici
- Piano (es.piano terra, primo piano) _____
- N. stanze _____
- Locali commerciali**
- N. stanze adibite al trattamento dati _____
- Descrizione (es.piano terra, primo piano) _____

12. Luogo dove sono custoditi gli archivi cartacei (es. fatture, buste paga, ecc.)

(indicare il luogo fisico dove è custodito l'archivio, es. uff. del Titolare, amministrazione, segreteria, magazzino, ecc.)

13. Sistemi di protezione delle aree e dei locali

Estintori Sistema di sorveglianza (custode, ...)

Allarme Sistema di video sorveglianza

Istituto di vigilanza Grate alle finestre

Armadi ignifughi

Cassaforte

Altro _____

Recinzione esterna Porte blindate

14. Sistema di video sorveglianza

Le immagini sono registrate SI NO

Su quale tipo di supporto HD Altro (specificare) _____

Indicare i soggetti incaricati a visionare le immagini di video sorveglianza: _____

Descrizione Impianto

Posizionamento apposita cartellonistica interna/esterna SI NO

N. videocamere installate:

Interne: _____ Esterne: _____

Posizionamento delle videocamere:

Interne: _____ Esterne: _____

Timbro e firma per accettazione
