PRIVACY

ASPETTI PRATICI

Athena

Reggio Emilia | 24 gennaio 2019

PRIVACY

Athena

PRIVACY

Legge 675/1996

D.Lgs.196/2003

Regolamento UE 679/2016
25 maggio 2018 (GDPR)

D.Lgs. 101 del 10/08/2018
IN VIGORE DAL 19/09/2018

D.Lgs. 101/2018

CONTINUITÀ

Il decreto legislativo contiene l'aggiornamento (massiccio) del **D.Lgs. 196/2003** (codice della PrivacY) che **rimane in vigore** (anche se molti articoli vengono abrogati o modificati sostanzialmente dal decreto).
Il D.Lgs. 101/2018 così come il D.Lgs. 196/2003 rimangono fonti SOTTO-ORDINATE rispetto al GDPR e quindi, in caso di contrasto o dubbio interpretativo, continuano a prevalere le disposizioni del GDPR.

D.Lgs. 101/2018

NOVITÀ

Nell'informativa non sono più presenti i riferimenti agli artt. 13 (informativa) e art. 7 (Diritti dell'interessato) del D.Lgs.196/2003 in quanto abrogati del D.L.101/2018. Resta il riferimento all'art.130 del D.Lgs.196/2003 (soft spam) in quanto non abrogato ma modificato del D.L.101/2018.

D.Lgs. 101/2018

DA RICORDARE

- Ai sensi dell'art. 6, comma 1 lettera b) Reg. UE 2016/679 **il consenso per adempimenti contrattuali o precontrattuali svolti su richiesta dell'interessato, non è richiesto**
- Ai sensi dell'art 130 comma 4 del D.Lgs.196/2003 come modificato dal D.L. 101/2018 è possibile utilizzare, senza chiedere il consenso all'interessato, i recapiti di posta elettronica forniti dal cliente all'atto della prestazione del servizio per l'invio di comunicazioni commerciali, a condizione che:
  - l'interessato non si opponga al momento che ne viene informato o anche successivamente
  - le comunicazioni siano riferite a prodotti o servizi analoghi a quelli forniti
  - le comunicazioni siano inviate dal Titolare che ha fornito il servizio

D.Lgs. 101/2018

DA RICORDARE

- Al di fuori del caso precedente è possibile l'invio di comunicazioni commerciali esclusivamente ai soggetti che hanno prestato uno specifico consenso
- La diffusione dei dati personali (tali sono le foto dell'immobile) necessita di preventivo consenso dell'interessato.

PRIVACY

SOGGETTI

INTERESSATO

PRIVACY
MINORI

Art. 50. Notizie o immagini relative a minori

1. Il **divieto** di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di **pubblicazione** e **divulgazione** con **qualsiasi mezzo** di **notizie** o **immagini idonee a consentire l'identificazione di un minore** si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale. La violazione del divieto di cui al presente articolo è punita ai sensi dell'**articolo 684 del codice penale**.

PRIVACY

OGGETTO DELLA TUTELA

Garanzia che i **trattamenti** dei **dati personali** rispettino i diritti e le libertà fondamentali e la dignità dell'interessato (riservatezza, identità personale, diritto alla protezione dei dati)

PRIVACY

TRATTAMENTO

Per trattamento di dati si intende **qualunque operazione** o complesso di operazioni, effettuati **anche senza** l'ausilio di **strumenti elettronici**, concernenti la **raccolta**, la **registrazione**, l'**organizzazione**, la **conservazione**, la **consultazione**, l'**elaborazione**, la **modificazione**, la **selezione**, l'**estrazione**, il **raffronto**, l'**utilizzo**, l'i**nterconnessione**, il **blocco**, la **comunicazione**, la **diffusione**, la **cancellazione** e la **distruzione** di dati, anche se non registrati in una banca di dati.

PRIVACY

DATI PERSONALI

Qualsiasi informazione riguardante una **persona fisica**, identificata o identificabile.

PRIVACY

CATEGORIE DI DATI PERSONALI

COMUNI

SENSIBILI

GIUDIZIARI

PRIVACY

DATI PERSONALI COMUNI

Non vi è necessità di consenso per il trattamento, salvo…

PRIVACY

DATI PERSONALI SENSIBILI

- **origine razziale ed etnica**
- opinioni politiche
- convinzioni filosofiche o religiose
- appartenenza sindacale
- dati genetici
- dati biometrici
- dati relativi alla **salute** o alla vita sessuale o all'**orientamento sessuale**

PRIVACY

DATI PERSONALI SENSIBILI

Il Regolamento Ue **vieta** il trattamento dei dati particolari a meno che…

- L'interessato ha prestato il proprio consenso
- …

PRIVACY
SOGGETTI

INTERESSATO

RESPONSABILE
DEL TRATTAMENTO

per specifici compiti, sotto l'autorità del titolare del trattamento

INCARICATO
DEL TRATTAMENTO

TITOLARE
DEL TRATTAMENTO

DPO

RESPONSABILI

Legge n. 167 del 20/11/2017 entrata in vigore il 12/12/2017
Modifica art. 29 del D.Lgs.196/2003

I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la **finalità perseguita**, la **tipologia dei dati**, la **durata del trattamento**, gli **obblighi e i diritti del responsabile** del trattamento e le **modalità di trattamento**;
i predetti atti sono adottati in conformità a schemitipo predisposti dal Garante»;

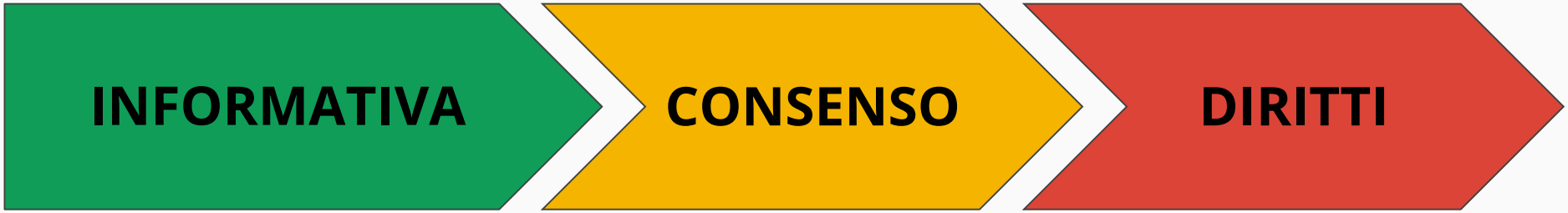
INCARICATI

Chiunque agisca sotto l'autorità del titolare del trattamento o del responsabile o abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.

INCARICHI SCRITTI
A DIPENDENTI E COLLABORATORI

PRIVACY

ADEMPIMENTI



INFORMATIVA - Cosa

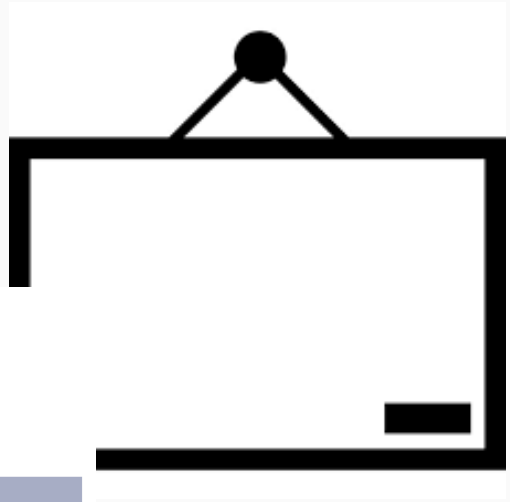
- CONCISA
- TRASPARENTE
- FACILMENTE COMPRENSIBILE ED ACCESSIBILE
- LINGUAGGIO CHIARO E SEMPLICE

INFORMATIVA - Contenuto

Informativa ai sensi degli art. 13 e 14 del Regolamento UE 679/2016 - Regolamento Generale sulla Protezione dei Dati (“RGPD”)

1. **TITOLARE** E (eventuale) DATA PROTECTION OFFICER
2. I **DATI** PERSONALI OGGETTO DI TRATTAMENTO
3. **FINALITA’**, BASE GIURIDICA E NATURA OBBLIGATORIA O FACOLTATIVA DEL TRATTAMENTO
4. **DESTINATARI**
5. **TRASFERIMENTI**
6. **CONSERVAZIONE** DEI DATI
7. I **DIRITTI** DELL INTERESSATO

INFORMATIVA - Come



INFORMATIVA - Cosa

CONSENSO - Cosa

- INFORMATO
- DIMOSTRABILE
- LIBERO
- SPECIFICO, CON RIFERIMENTO A TRATTAMENTI CHIARAMENTE INDIVIDUATI
- REVOCABILE

CONSENSO - Quando

NO	SI
• incarico di ricerca o mediazione, anche prima della sottoscrizione di un contratto o mandato	• **marketing** • **comunicazione / diffusione** • dati sensibili • profilazione

COMUNICAZIONE

Il dare conoscenza dei dati personali **a uno o più soggetti determinati** diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, **in qualunque forma**, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione

DIFFUSIONE

Il dare conoscenza dei dati personali **a soggetti indeterminati**, **in qualunque forma**, anche mediante la loro messa a disposizione o consultazione

CONSENSO

Art. 6 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
   a. **l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;**
   b. **il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;**
   c. ...
   d. ...
   e. ...
   f. ...

CONSENSO

Art. 7 - Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, **il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso** al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è **prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile** dalle altre materie, in **forma comprensibile** e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

CONSENSO

Art. 7 - Condizioni per il consenso

3. L'interessato ha il **diritto di revocare il proprio consenso** in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la **prestazione di un servizio**, sia **condizionata alla prestazione del consenso** al trattamento di dati personali **non necessario** all'esecuzione di tale contratto.

DOPO IL TRATTAMENTO

L'articolo 99 chiarisce che, una volta **esaurita la finalità** o la condizione di liceità del trattamento (es. revoca del consenso) è **ammessa** la **conservazione** dei dati (non l'ulteriore trattamento!) a determinate condizioni di cui all'art. 89 del GDPR:
Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

SITO WEB Agenzia

SITO WEB Agenzia

INFORMATIVA PRIVACY

PRIVACY POLICY

COOKIE POLICY

PRIVACY POLICY

- **Informa gli utenti del sito dell'uso dei dati personali (IP) e dei soggetti che possono venire a conoscenza dei dati.**
- **Deve essere indicato l'eventuale responsabile esterno (azienda che cura la parte tecnologica del sito)**
- **Deve essere visualizzabile in tutte le pagine del sito**

COOKIE POLICY

I siti web generalmente **utilizzano cookie.**
I cookie sono file di informazioni che i siti web memorizzano **sul computer dell'utente** di Internet durante la navigazione, spec. allo scopo di identificare chi ha già visitato il sito in precedenza.

I Cookie possono essere di diverse tipologie, funzionali, tecnici o di profilazione.


GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
Il tuo sito/blog installa cookie? Cosa devi fare
IMPORTANTE: per una corretta interpretazione degli adempimenti previsti, si raccomanda la consultazione del Provvedimento del Garante dell'8 maggio 2014 e dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie».
I documenti sono disponibili su www.garanteprivacy.it/cookie
Segnalarli nell'informativa
Art .2, par. 5, Direttiva 2009/136/CE e art. 122, comma 1, Codice privacy
Inserire il banner e richiedere il consenso ai visitatori
Art .2, par. 5, Direttiva 2009/136/CE e art. 122, comma 1, Codice privacy
Notificare al Garante
Art. 37, comma 1, lett. d), Codice privacy
CHE TIPO DI COOKIE INSTALLI?
LEGENDA: adempimento previsto adempimento non previsto
Nessun cookie
Tecnici o analitici prima parte
Analitici terze parti
(se sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) – vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»
Analitici terze parti
(se NON sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) – vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»
Di profilazione prima parte
Di profilazione terze parti
La notificazione è a carico del soggetto terza parte che svolge l'attività di profilazione

CLOUD

- Il titolare del trattamento dei dati personali che trasferisce in tutto o in parte il trattamento sulle nuvole deve designare il fornitore del servizio cloud “responsabile del trattamento”
- In caso di violazioni commesse dal fornitore anche il titolare sarà’ chiamato a rispondere dell’eventuale illecito
- Necessità’ di esercitare un controllo effettivo nei confronti del cloud provider e sulle modalità’ di gestione dei dati

CLOUD

- Assicurarsi che siano adottate misure tecniche ed organizzative volte a ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito.
- Accertarsi che i dati siano sempre disponibili (che si possa sempre accedere ad essi)
- Accertarsi che i dati siano riservati (che l'accesso sia consentito solo a chi ne ha diritto)

CLOUD

- Informarsi su dove risiederanno i propri dati: in italia, in europa o in un paese extraeuropeo?

CLOUD

INFORMARSI SU DOVE RISIEDERANNO I PROPRI DATI: IN ITALIA, IN EUROPA O IN UN PAESE EXTRAEUROPEO?

- i dati personali possono circolare liberamente entro l'unione europea
- il Regolamento UE definisce regole precise per il trasferimento di dati personali fuori dall'unione europea
- per trasferire dati al di fuori dell'unione europea devono essere garantiti standard di protezione adeguati a quelli europei

CONSENSO e MARKETING

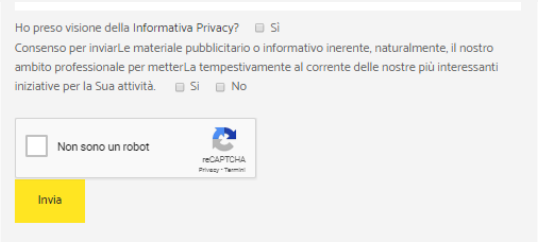
Ho preso visione della Informativa Privacy? ☐ Sì

Consenso per inviarLe materiale pubblicitario o informativo inerente, naturalmente, il nostro ambito professionale per metterLa tempestivamente al corrente delle nostre più interessanti iniziative per la Sua attività. ☐ Si ☐ No

Non sono un robot

reCAPTCHA
Privacy - Termini

Invia



TRATTAMENTO e MARKETING

DATO	ATTIVITÀ
Numeri telefonici ed indirizzi presenti in **elenchi telefonici**	Mediante l'uso del telefono con operatore e mediante posta cartacea: • **a prescindere dal consenso** dell'interessato • **salvo il diritto di opposizione** (iscrizione nel registro pubblico delle opposizioni)

TRATTAMENTO e MARKETING

DATO	ATTIVITÀ
Numeri telefonici ed indirizzi presenti in **elenchi pubblici** (es. albi o camera di commercio)	Mediante l'uso del telefono con operatore e mediante posta cartacea: • **a prescindere dal consenso** dell'interessato • **salvo il diritto di opposizione** • **FATTO SALVO IL VINCOLO DI FINALITÀ**

TRATTAMENTO e MARKETING

DATO	ATTIVITÀ
Numeri telefonici ed indirizzi di posta elettronica	Mediante l'uso di strumenti automatizzati (posta elettronica, telefax, mms, sms, telefonate automatizzate senza operatore) • **SOLO CON PREVENTIVO CONSENSO ESPRESSO DELL'INTERESSATO**

CONSENSO

I requisiti di validità del consenso per l'invio di comunicazioni promozionali:

- **INFORMATO**
- **LIBERO**
- **SPECIFICO, CON RIFERIMENTO A TRATTAMENTI CHIARAMENTE INDIVIDUATI**
- **DIMOSTRABILE**

SOFT SPAM AI PROPRI CLIENTI

Il Provv. del 19/6/2008 consente ai soggetti che hanno venduto un prodotto o prestato un servizio di inviare via **e-mail o posta tradizionale** comunicazioni commerciali, purché:

- Ci si rivolga a soggetti cui si è già venduto un prodotto o un servizio
- L'attività promozionale riguardi beni o servizi del medesimo titolare e analoghi a quelli oggetto della precedente vendita
- L'interessato sia informato della possibilità di opporsi in qualsiasi momento al trattamento
- L'interessato non si sia opposto sin dall'inizio o successivamente

MAILING LIST

- L’attività promozionale effettuata utilizzando liste di e-mail in chiaro, che permette ai destinatari del messaggio di conoscere chi sono gli altri destinatari del messaggio e pertanto di conoscere ed utilizzare i loro indirizzi mail **NON È MAI CONSENTITA**
- E’ necessario mantenere riservati gli indirizzi di posta utilizzati per l’invio del messaggio promozionale, ad esempio utilizzando la funzione “ccn” copia conoscenza nascosta o attraverso strumenti dedicati: Mailchimp, MailUp, ...

SOCIAL SPAM

- L’agevole rintracciabilità di dati personali in Internet **non autorizza** a poter utilizzare tali dati per inviare comunicazioni promozionali automatizzate **senza il consenso** dei destinatari
- I **messaggi promozionali** inviati agli utenti di social network (come Facebook), in privato o pubblicamente sulla propria bacheca virtuale, sono sottoposti alla disciplina del **Codice Privacy**

SOCIAL SPAM - Esempi

IMPRESA CHE TRAE I DATI PERSONALI DI UN SOGGETTO DAL PROFILO DEL SOCIAL NETWORK A CUI E' ISCRITTO E INVIA COMUNICAZIONE PROMOZIONALE IN PRIVATO O IN BACHECA O ALL'INDIRIZZO MAIL COLLEGATO AL PROFILO

TRATTAMENTO **ILLECITO** SALVO CHE SI DIMOSTRI DI AVER ACQUISITO UN CONSENSO PREVENTIVO INFORMATO SPECIFICO LIBERO E DOCUMENTATO

UTENTE CHE DIVENTA FAN DELLA PAGINA DI UN'IMPRESA O FOLLOWER DI UN MARCHIO O PRODOTTO E SUCCESSIVAMENTE NE RICEVE MESSAGGI PROMOZIONALI

TRATTAMENTO **LECITO** SOLO SE DAL CONTESTO O DALLE MODALITÀ' DI FUNZIONAMENTO DEL SOCIAL NETWORK SI EVINCE CHIARAMENTE CHE L'INTERESSATO ABBIA VOLUTO MANIFESTARE ANCHE LA VOLONTÀ DI FORNIRE IL PROPRIO CONSENSO ALLA RICEZIONE DI MESSAGGI PROMOZIONALI

MISURE DI SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

MISURE DI SICUREZZA

- Pseudoanonimizzazione
- Riservatezza
- Integrità e disponibilità dei dati su base permanente, resilienza dei sistemi e dei servizi
- Capacità di ripristino dei dati
- Procedure per testare il ripristino dei dati

ACCOUNTABILITY

Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per **garantire ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al regolamento.
Dette misure sono riesaminate e aggiornate qualora necessario

ADEGUAMENTO AL REGOLAMENTO

PRIVACY BY DESIGN - PRIVACY BY DEFAULT

Il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, **solo i dati necessari per ogni specifica attività di trattamento**.
Tale obbligo vale per la **quantità** dei dati personali raccolti, la **portata** del trattamento , il **periodo** di conservazione, e l'**accessibilità**.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Raccomandazione del Garante Italiano sul Registro dei trattamenti:

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Soggetti obbligati alla tenuta:

- Titolari del trattamento
- Responsabili del trattamento

Solo se:

- più di 250 dipendenti
- trattamenti che presentino un rischio per i diritti e le libertà dell'interessato
- categorie particolari di dati (art.9)
- dati giudiziari (art. 10)

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

FAQ del Garante - https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);

- liberi professionisti con al
  reati (es. commercialisti,
- associazioni, fondazioni e
  reati (i.e. organizzazioni d
  persone con disabilità, ex
  discriminazioni di genere
  sportive con riferimento
  carattere religioso);
- il condominio ove tratti "
  all'abbattimento delle ba
  comprensive di spese me

Al di fuori dei casi di tenuta obbligatoria del Registro, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[Indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Contenuto del registro:

- Titolare ed eventuale contitolare
- Finalità del trattamento
- Categorie di interessati
- Categorie di destinatari
- Trasferimenti verso paesi terzi
- Tempi per la cancellazione dati
- Misure di sicurezza adottate

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Finalità del trattamento:

- nel campo “finalità del trattamento” oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del RGPD; in merito, con particolare riferimento al “legittimo interesse”, si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le “garanzie adeguate” eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d’impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018 – [doc web n. 8080493]). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di “categorie particolari di dati”, indicare una delle condizioni di cui all’art. 9, par. 2del RGPD; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell’Unione europea) che ne autorizza il trattamento ai sensi dell’art. 10 del RGPD;

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Categorie di interessati:

- nel campo “descrizione delle categorie di interessati e delle categorie di dati personali” andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Categorie di destinatari:

- nel campo “categorie di destinatari a cui i dati sono stati o saranno comunicati” andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Trasferimenti verso paesi terzi:

- nel campo "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);

Tempi per la cancellazione dati:

- nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Trasferimenti verso paesi terzi:

- nel campo “descrizione generale delle misure di sicurezza” andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell’art. 32 del RGDP tenendo presente che l’elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l’Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l’insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Modalità di conservazione e di aggiornamento:

- Il Registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro.
- Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione unitamente a quella dell'ultimo aggiornamento.

VIOLAZIONE DATI PERSONALI - DATA BREACH

IL TITOLARE:

- NOTIFICA ALL'AUTORITÀ' DI CONTROLLO
  - Ove possibile entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza
  - Se fatta oltre le 72 ore deve contenere motivi del ritardo
- DOCUMENTA la violazione, le circostanze ad essa relative, le conseguenze ed i provvedimenti adottati

VIOLAZIONE DATI PERSONALI - DATA BREACH

Contenuto della notifica:

- Natura della violazione
- Ove possibile, categorie e numero di interessati e di registrazioni di dati personali coinvolti
- Nome e dati di contatto del responsabile della protezione dei dati o altro soggetto di riferimento
- Descrizione probabili conseguenze della violazione
- Descrizione misure adottate o da adottare per porre rimedio alla violazione e attenuarne effetti negativi

VIOLAZIONE DATI PERSONALI - DATA BREACH

L'obbligo di **comunicazione all'interessato** della violazione viene meno se:

- Erano state applicate ai dati oggetto della violazione misure di sicurezza adeguate, in particolare quelle idonee a renderli incomprensibili (es, la cifratura)
- Il titolare del trattamento ha adottato in seguito alla violazione misure idonee ad evitare il sopraggiungere di un rischio elevato per i diritti e le libertà personali
- Tale comunicazione richiederebbe sforzi sproporzionati. In tal caso si dovrà fare una comunicazione pubblica

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (PIA)

Obbligatoria se:

- Il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (PIA)

Richiesta in particolare se ...

- Valutazione sistematica e globale di aspetti personali relative a persone fisiche (profilazione)
- Trattamento su larga scala di dati personali particolari (art. 9 e art.10)
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

E’ designato in funzione:

- Delle qualità professionali
- Della capacità di assolvere ai compiti indicati dall’art. 39

Può essere:

- Un dipendente del titolare o del responsabile
- Può svolgere i suoi compiti sulla base di un contratto di servizi

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

È obbligatoria la designazione:

a. se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
b. se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
c. se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati .

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Compiti del DPO

- Consulenza sugli obblighi derivanti dal regolamento
- Sorvegliare l'osservanza del Regolamento
- Fornire pareri sulla PIA e sorvegliare lo svolgimento
- Fungere da contatto con l'autorità di controllo

SANZIONI AMMINISTRATIVE

Sanzioni pecuniarie fino a € **20.000.000** o, per le imprese, fino al **4%** del fatturato mondiale annuo	• Violazione dei principi del trattamento, comprese le condizioni di consenso • Diritti degli interessati • Trasferimento verso un paese terzo • Qualsiasi obbligo ai sensi delle legislazioni degli stati membri
Sanzioni pecuniarie fino a € **10.000.000** o, per le imprese, fino al **2%** del fatturato mondiale annuo	• Violazione degli obblighi del titolare del trattamento • Obblighi dell'organismo di certificazione • Obblighi dell'organismo di controllo

SANZIONI PENALI

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento dì cui all'articolo 129 arreca nocumento all'interessato, è punito con la **reclusione** da **sei mesi** a un anno e sei mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2- octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la **reclusione** da **uno** a tre **anni**.

SANZIONI PENALI

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
4. Il Pubblico Ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.
6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

SANZIONI PENALI

Art. 167-bis. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la **reclusione** da **uno** a sei **anni**.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la **reclusione** da **uno** a sei **anni**, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.
3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

SANZIONI PENALI

Art. 167-ter. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la **reclusione** da **uno** a quattro **anni**.
2. Per il reato dì cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

RECLAMI AL GARANTE

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4535524

RIEPILOGANDO

RIEPILOGANDO

- **Ricognizione dei trattamenti: cosa, chi, come e quando** (Accountability, analisi dei rischi, azioni correttive, formazione del personale)
- **Aggiornare le informative ed i consensi** (clienti, dipendenti e collaboratori)
- **Modificare i contratti con i soggetti cui si affidano i dati inserendo le informazioni obbligatorie per il trattamento** (nomine Responsabili del trattamento)
- **Istruire per iscritto gli incaricati del trattamento** (dipendenti e collaboratori)
- Verificare ed adeguare sito web (informtiva, privacy policy, cookie policy, consensi)
- **Registri del trattamento**

LA MODULISTICA FEDERATIVA

MODULISTICA

INFORMATIVA CLIENTI

INFORMATIVA DIPENDENTI

NOMINA RESPONSABILE

GUIDA PRIVACY

COSA E QUANDO

WEB

QUANDO	COSA
NAVIGATORE CONSULTA IL SITO	• Trova su tutte le pagine i link all'informativa, alla privacy policy ed alla cookie policy
NAVIGATORE COMPILA UNA FORM	• Esprime il suo consenso informato, specifico e libero al trattamento dei dati a fini marketing
DESTINATARIO RICEVE UNA MAIL	• Trova il link all'informativa nella firma della mail

IN AGENZIA

QUANDO	COSA
CLIENTE CI FORNISCE INCARICO DI RICERCA	• Trova esposta l'informativa privacy • Può ottenere copia dell'informativa
CLIENTE CI FORNISCE INCARICO DI VENDITA	• Trova esposta l'informativa privacy • Può ottenere copia dell'informativa • Esprime il suo consenso informato, specifico e libero al trattamento dei dati a fini marketing e diffusione

FUORI AGENZIA

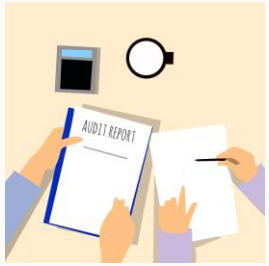
QUANDO	COSA
CLIENTE CI FORNISCE INCARICO DI RICERCA	• Può ottenere copia dell'informativa
CLIENTE CI FORNISCE INCARICO DI VENDITA	• Può ottenere copia dell'informativa • Esprime il suo consenso informato, specifico e libero al trattamento dei dati a fini marketing e diffusione

Cosa fa FIAIP

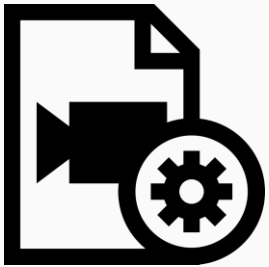
Cosa fa FIAIP

MODULISTICA

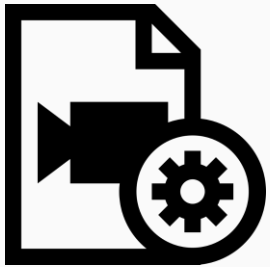
GUIDA



CONSULENZA PERSONALIZZATA



WEBINAR GDPR



WEBINAR OPERATIVO

SOFTWARE EXPERT

CONSULENZA PRIVACY PERSONALIZZATA

GRAZIE!