Il Regolamento Europeo sulla protezione dei dati

GDPR

Athena

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)

Athena

Dalla 675/96 al Regolamento Ue

- Legge 675/1996
  - D.Lgs.196/2003
    - Regolamento UE 679/2016, applicabile dal **25 maggio 2018**

Athena

D.Lgs.101/2018

Pubblicato in G.U. il 08.08.2018

Entrato in vigore il 19.09.2018

ARMONIZZAZIONE CODICE DELLA PRIVACY AL REG. UE

Athena

I numeri del Garante nel 2017

- Riscontro a 6.000 reclami e segnalazioni
- Decisi 276 ricorsi
- Effettuate 275 ispezioni
- 41 Violazioni segnalate all'Autorità Giudiziaria per mancata adozione delle misure di sicurezza e protezione dei dati e trattamento illecito
- 589 Violazioni amministrative contestate
- Riscosse sanzioni amministrative per circa 3 milioni e 800 mila euro

Athena

(Relazione annuale Garante Privacy 2017)

GDPR – AMBITO DI APPLICAZIONE

- Trattamenti parzialmente o totalmente automatizzati e trattamenti non automatizzati di dati personali
  - ESCLUSIONI
    - Trattamenti effettuati da persona fisica per attività a carattere esclusivamente domestico o personale
    - Trattamenti effettuati dalle Autorità nel perseguimento dei reati

Cosa è il TRATTAMENTO:

qualunque operazione o complesso di operazioni effettuate 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'interconnessione
- Il blocco
- La comunicazione
- La diffusione
- La cancellazione
- La distruzione

Cosa intendiamo per dato personale?

Qualsiasi informazione riguardante un persona fisica, identificata o identificabile

Athena

Quali elementi rendono identificabile una persona fisica?

- Nome
- Un numero di identificazione
- Dati relativi all'ubicazione
- Identificativo on line
- Uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Athena

Le categorie di dati personali

- Dati comuni
- Dati sensibili
- Dati giudiziari

- **Dati particolari:**
  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
- **Dati relativi a condanne penali**
- **Dati Comuni**

Athena

Studio Athena di S. Algerio- riproduzione riservata

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

- L'interessato ha prestato il proprio **consenso**
- Il trattamento sia necessario per assolvere obblighi in materia di diritto del lavoro o sicurezza sociale e protezione sociale
- **Il trattamento è effettuato da un'associazione o fondazione che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con l'organismo a motivo delle sue finalità e i dati non siano comunicati all'esterno**
- Il trattamento riguardi dati resi manifestamente pubblici dall'interessato
- Il trattamento è necessario per finalità di medicina preventiva, del lavoro o valutazione della capacità lavorativa, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali

Studio Athena di S. Algerio- riproduzione riservata

Ambito soggettivo del trattamento

Athena

Titolare del trattamento

- Persona fisica, giuridica ente o associazione che determina modalità e finalità del trattamento ed i profili della sicurezza

Responsabile del trattamento

- Soggetto cui il Titolare affida il trattamento dei dati

Incaricato del trattamento

- Soggetto autorizzato a svolgere operazioni di trattamento che opera sotto il controllo e l'autorità del Titolare

Athena

Responsabile della Protezione dati

D.P.O

Athena

E' designato in funzione:

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

Athena

Può essere:

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

Athena

Quando 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;
oppure
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 .

Athena

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

Athena

Informativa

Artt. 13 e 14 Regolamento Ue 679/2016

Ex art. 13 D. Lgs.196/2003 – abrogato -

Athena

Quando e come

Athena

L'informativa.....

- Concisa
- Trasparente
- Facilmente comprensibile e accessibile
- Linguaggio chiaro e semplice

Athena

- **L'informativa può essere resa disponibile affiggendola in luogo visibile**

- **Può essere resa disponibile mediante link nelle email :**

Studio Athena di S. Algerio
Via Cinque Fonti, 2
05022 Amelia (Tr)
Tel. 0744 982181
Informativa ex art. 13 Reg. UE 679/2016
http://www.athenaconsul.it/Informativa.pdf

Athena

Contenuto dell'informativa

- Informativa ai sensi dell'artt. 13 e 14 del Regolamento UE 679/2016 Regolamento Generale sulla Protezione dei Dati ("RGPD")

1. **TITOLARE E DATA PROTECTION OFFICER**
2. **I DATI PERSONALI OGGETTO DI TRATTAMENTO**
3. **FINALITA', BASE GIURIDICA E NATURA OBBLIGATORIA O FACOLTATIVA DEL TRATTAMENTO**
4. **MODALITA' DEL TRATTAMENTO**
5. **ACCESSO AI DATI E COMUNICAZIONE DEI DATI**
5. **TRASFERIMENTI**
6. **CONSERVAZIONE DEI DATI**
7. **DIRITTI DELL INTERESSATO E MODALITA' DI ESERCIZIO**

LA BASE GIURIDICA DEL TRATTAMENTO…..

Articolo 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 contrat**to di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;

c)il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d)il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e)il trattamento è 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;

f)il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
a)dal diritto dell'Unione; o
b)dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

I DIRITTI DELL'INTERESSATO

- Diritto di accesso
- Diritto di rettifica o cancellazione
- Diritto di limitazione del trattamento o di opposizione
- Diritto alla portabilità
- Diritto di oblio
- Diritto di reclamo all'Autorità di controllo

Athena

L'Autorizzazione generale 3/2016

Autorizzazione al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni

Athena

AUTORIZZA

- il trattamento dei dati sensibili di cui all´art. 4, comma 1, lett. d), del Codice da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo……

Athena

Ambito di applicazione.

- *a) alle associazioni anche non riconosciute, ai partiti e ai movimenti politici, alle associazioni e alle organizzazioni sindacali, ai patronati e alle associazioni di categoria, alle casse di previdenza, alle organizzazioni assistenziali o di volontariato, nonché alle federazioni e confederazioni nelle quali tali soggetti sono riuniti in conformità, ove esistenti, allo statuto, all´atto costitutivo o ad un contratto collettivo;*
- *b) alle fondazioni, ai comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, ivi comprese le organizzazioni non lucrative di utilità sociale (Onlus);*
- *c) alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818……*

Finalità

- L´autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dalla legge, dall´atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell´insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell´ambiente e delle cose d´interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

Athena

Finalità

- Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell´associazione, della fondazione, del comitato o del diverso organismo, o per l´adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.
- Qualora i soggetti di cui alle lettere a), b) e c) del punto 1 si avvalgano di persone giuridiche o di altri organismi con scopo di lucro o di liberi professionisti per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi, persone giuridiche o liberi professionisti

Athena

Interessati cui si riferiscono i dati

- Il trattamento può riguardare i dati sensibili attinenti:
- a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 2), ai relativi familiari e conviventi;
- b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l´associazione, la fondazione o il diverso organismo;
- c) ai soggetti che ricoprono cariche sociali o onorifiche;
- d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall´associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all´atto costitutivo, ove esistenti, o comunque a coloro nell´interesse dei quali i soggetti menzionati al punto 1) possono operare in base ad una previsione normativa;
- e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;
- f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l´adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

Athena

Categoria di dati oggetto del trattamento

- L´autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l´**autorizzazione generale n. 2/2016**.

Athena

Autorizzazione generale 2/2016

Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

Athena

a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell´interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle relazioni tra i fattori di rischio e la salute umana anche con riguardo a studi nell´ambito della sperimentazione clinica di farmaci, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull´utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. In tali casi, il trattamento può comprendere anche dati idonei a rivelare la vita sessuale e l´origine razziale ed etnica solo ove indispensabili per il raggiungimento delle finalità della ricerca. Inoltre, occorre acquisire il consenso (in conformità a quanto previsto dagli artt. 106, 107 e 110 del Codice), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l´abbinamento al materiale di ricerca dei dati identificativi dell´interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima. Resta fermo quanto previsto dall´art. 98 del Codice;

Athena

b) alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;
c) alle comunità di recupero e di accoglienza, alle case di cura e di riposo, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;
d) agli enti, alle associazioni e alle organizzazioni religiose riconosciute, relativamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi nei limiti di quanto stabilito dall´art. 26, comma 4, lett. a), del Codice, fermo restando quanto previsto per le confessioni religiose dagli articoli 26, comma 3, lett. a), e 181, comma 6, del Codice e dall´autorizzazione n. 3/2016;

Athena

e) alle persone fisiche o giuridiche, alle imprese, anche sociali, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati, ove necessario attinenti anche alla vita sessuale, e alle operazioni indispensabili per adempiere agli obblighi, anche precontrattuali, derivanti da un rapporto di fornitura all´interessato di beni, di prestazioni o di servizi.
Se il rapporto intercorre con imprese assicurative o istituti di credito, devono considerarsi indispensabili i soli dati ed operazioni strettamente necessari per fornire specifici prodotti o servizi richiesti dall´interessato. Il rapporto può riguardare anche la fornitura di strumenti di ausilio per la vista, per l´udito o per la deambulazione;

f) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi che gestiscono impianti o strutture sportive, limitatamente ai dati idonei a rivelare lo stato di salute e alle operazioni indispensabili per accertare l´idoneità fisica alla partecipazione ad attività sportive o agonistiche;

Athena

IL CONSENSO

Athena

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.**

Athena

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.

Athena

....LA PROMOZIONE E LA RACCOLTA FONDI

LINEE GUIDA IN MATERIA DI ATTIVITA' PROMOZIONALE E CONTRASTO ALLO SPAM
Provvedimento del 4 luglio 2013

NUOVE DISPOSIZIONI IN MATERIA DI ISCRIZIONE E FUNZIONAMENTO DEL REGISTRO DELLE OPPOSIZIONI
Legge n. 5 del 11 gennaio 2018

IL TRATTAMENTO DEI DATI PER FINALITA' DI MARKETING

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)

REGISTRO PUBBLICO DELLE OPPOSIZIONI - L. 5/2018 (in vigore dal 4 febbraio 2018)

- ✓ Utenze telefoniche fisse e mobili
- ✓ Opposizioni al trattamento delle proprie numerazioni telefoniche effettuato mediante operatore con l'impiego del telefono per fini pubblicitari, di vendita diretta, compimento di ricerche di mercato o comunicazioni commerciali
- ✓ **Con l'iscrizione si intendono revocati tutti i consensi precedentemente espressi**
- ✓ Sono fatti salvi i consensi prestati nell'ambito di un rapporto contrattuale in essere, o cessato da non più di 30 giorni, aventi ad oggetto la fornitura di beni o di servizi
- ✓ E' valido il consenso al trattamento dei dati personali prestato dall'interessato successivamente all'iscrizione nel registro
- ✓ Vietata la comunicazione a terzi di dati personali degli interessati iscritti al registro
- ✓ **Il titolare del trattamento è responsabile in solido delle violazioni anche nel caso di affidamento a terzi di attività di call center per l'effettuazione delle chiamate telefoniche**
- ✓ Gli operatori che utilizzano i sistemi di pubblicità o vendita telefonica hanno l'obbligo di consultare mensilmente, e comunque prima dell'inizio di ogni nuova campagna promozionale, il registro pubblico delle opposizioni.

Studio Athena di S. Algerio- riproduzione riservata

Sanzioni

- Violazione del diritto di opposizione
- Violazione del divieto di comunicare a terzi, trasferire e diffondere dati personali degli iscritti al registro, per finalità di pubblicità o vendita
  - Sanzione amministrativa da 10mila a 120mila euro

IL TRATTAMENTO DEI DATI PER FINALITA' DI MARKETING

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 FINALITA'

IL TRATTAMENTO DEI DATI PER FINALITA' DI MARKETING

MEDIANTE L'USO DI STRUMENTI AUTOMATIZZATI (POSTA ELETTRONICA, TELEFAX, MMS, SMS, TELEFONATE AUTOMATIZZATE SENZA OPERATORE)

- PREVENTIVO CONSENSO ESPRESSO DELL'INTERESSATO

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

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

UTILIZZO DI MAILING LIST

- L'attività promozionale effettuata utilizzando liste di e-mail in chiaro, permette ai destinatari del messaggio di conoscere chi sono gli altri destinatari del messaggio e pertanto di conoscere ed utilizzare i loro indirizzi mail
- E' necessario mantenere riservati gli indirizzi di posta utilizzati per l'invio del messaggio promozionale (ad esempio utilizzando la funzione "ccn" copia conoscenza nascosta)

IL *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

Studio Athena di S. Algerio- riproduzione riservata

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 MODALITA' DI FUNZIONAMENTO DEL SOCIAL NETWORK SI EVINCE CHIARAMENTE CHE L'INTERESSATO ABBIA VOLUTO MANIFESTARE ANCHE LA VOLONTA' DI FORNIRE IL PROPRIO CONSENSO ALLA RICEZIONE DI MESSAGGI PROMOZIONALI

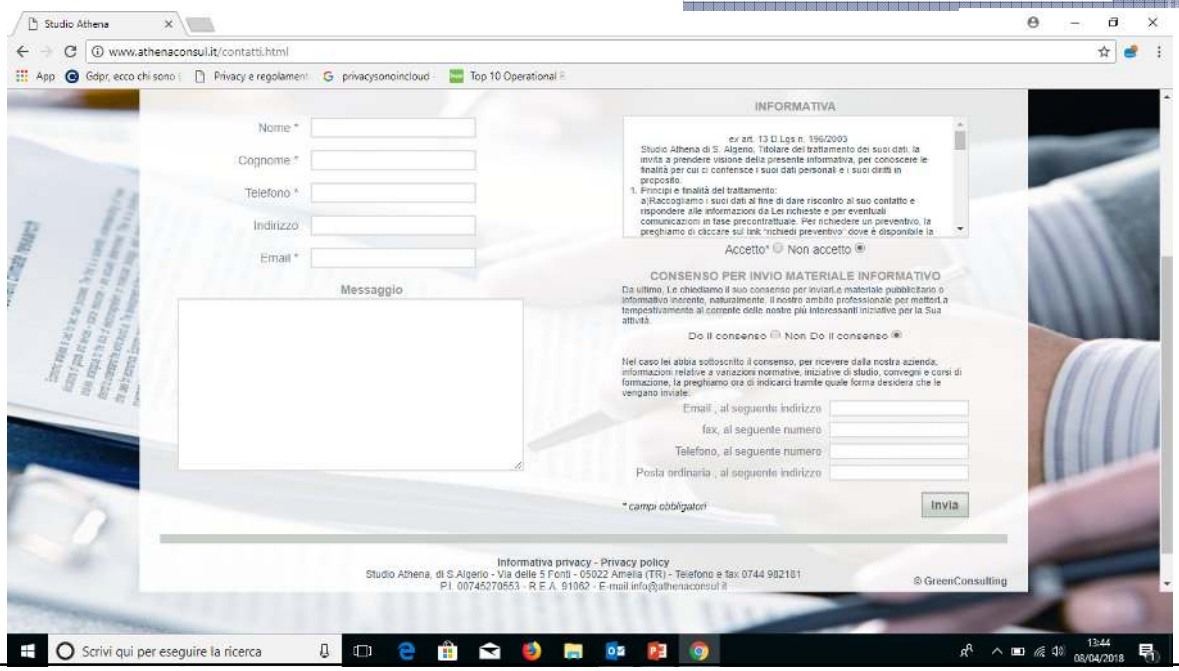
Il sito web

Athena

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) e dove sono trattati i dati.
Deve esser visualizzabile in tutte le pagine del sito.

I siti web 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.

Athena



IL CLOUD COMPUTING

Athena

COSA E' UNA NUVOLA INFORMATICA?

UN INSIEME DI TECNOLOGIE, DI SOLITO SOTTO FORMA DI UN SERVIZIO OFFERTO DA UN PROVIDER AL CLIENTE, CHE PERMETTONO DI MEMORIZZARE, ARCHIVIARE E/O ELABORARE DATI NON PIU' SUL PROPRIO COMPUTER, MA IN RETE, SUI SISTEMI DEL FORNITORE

Athena

LA PRIVACY NELLE NUVOLE

- 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 SARA' CHIAMATO A RISPONDERE DELL'EVENTUALE ILLECITO
- NECESSITA' DI ESERCITARE UN CONTROLLO EFFETTIVO NEI CONFRONTI DEL CLOUD PROVIDER E SULLE MODALITA' DI GESTIONE DEI DATI

- 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)

Athena

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

Athena

- 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

Athena

Il Responsabile del trattamento

Art.28 Regolamento UE 679/2016

Athena

Responsabili del trattamento, ad esempio….

- Commercialista
- Soggetto incaricato della manutenzione del sito web
- Consulente del Lavoro
- Soggetto cui sono affidati i dati in cloud

Il Titolare del trattamento può affidare dati

- Unicamente a responsabili del trattamento che presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 679/2016 e garantisca la tutela dell'interessato

Athena

Nomina del Responsabile

- Disciplinata **da un contratto o da altro atto giuridico** a norma del diritto dell'unione o degli altri Stati membri che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, **la natura** e la **finalità** del trattamento, il **tipo di dati personali** e le **categorie di interessati**, gli **obblighi e i diritti** del titolare del trattamento.

Athena

Il contratto prevede in particolare che il responsabile del trattamento..

Athena

- Tratti i dati soltanto su istruzione documentata del titolare
- Garantisca che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza
- Adotti tutte le misure ai sensi dell'art. 32
- Non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento
- Assista il titolare nel rispetto degli obblighi del regolamento
- Su scelta del titolare cancelli o restituisca tutti i dati al termine della prestazione
- Metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente articolo e consenta l'attività di revisione ed ispezione del titolare

Athena

Visto l'art. 28 del Regolamento UE 679/2016

Considerato che ..... presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 679/2016 e garantisca la tutela dei diritti dell'interessato.

Ad integrazione del contratto stipulato in data ..... le parti concordano quanto segue:

A. Il responsabile del trattamento può avvalersi/non può avvalersi di un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

B. I dati oggetto del contratto richiamato saranno trattati per il perseguimento delle seguenti finalità:.....-

C. Il trattamento sarà svolto dal..... al.....

D. Il responsabile del trattamento tratterà i dati personali soltanto su istruzione documentata del titolare, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda una disposizione normativa;

E. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

F. Il Responsabile del trattamento adotta tutte le misure richieste ai sensi dell'art. 32 del Reg.UE 679/2016

G. Il Responsabile del trattamento si impegna ad assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare de trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

H. Il Responsabile del Trattamento si impegna ad assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;

I. Il Responsabile del Trattamento, al termine della prestazione contrattuale, si impegna a (cancellare/restituire) tutti i dati personali relativi ai trattamenti effettuati, nonché a cancellare le copie esistenti salvo il caso in cui la conservazione da parte del Responsabile sia prevista dal diritto dell'Unione o degli Stati membri.

J. Il Responsabile del Trattamento metterà a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi dell'art.28 Reg.UE 679/2016 e consentirà e contribuirà alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato.

K. Il responsabile del trattamento informerà immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione ricevuta violi il Regolamento UE/679/2016 o altre disposizioni, nazionali o dell'Unione relative alla protezione dei dati.

Athena

Gli incaricati del trattamento

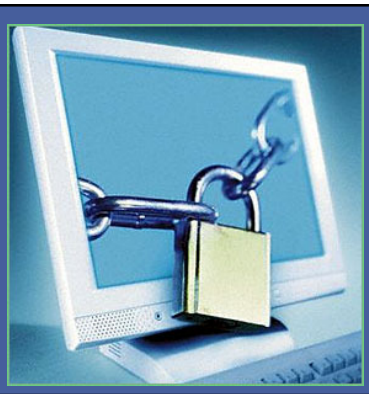
Athena

Incaricati del trattamento

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.

Athena

LA SICUREZZA DEI DATI



Dal D.LGS.196/2003 AL REG.UE 679/2016

Athena

Codice Privacy

Misure Idonee

- Art.31

Misure Minime

- Art.33-34-35

Athena

Il principio di ACCOUNTABILITY nel Reg. UE

Athena

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 presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario

Athena

Procedura per adeguamento Privacy

Athena

Le misure devono Garantire

- Pseudo anonimizzazione e cifratura
- Capacità di assicurare : riservatezza, integrità, disponibilità e resilienza dei sistemi
- Procedura di verifica e valutazione misure di sicurezza
- Analisi dei rischi
- Adesione a Codici di Condotta

Athena

PRIVACY BY DESIGN e PRIVACY BY DEFAULT

Art. 25 Regolamento Ue

Athena

Il titolare del trattamento mette in atto, fin dalla progettazione, misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica attività di trattamento.

- Ridurre al minimo il trattamento dei dati personali

Athena

Qualche esempio di misure tecniche ed organizzative…

Athena

Per il trattamento dei dati con modalità cartacea:

- Informativa preventiva
- Consenso
- Lettera di incarico/istruzione ai soggetti autorizzati
- Nomina Responsabili
- Conservazione dei dati in modo da prevenire accessi non autorizzati o distruzione dei dati stessi.
- Previsione di procedure per la conservazione degli atti in archivi ad accesso selezionato

Studio Athena di S. Algerio- riproduzione riservata

Trattamento dei dati con strumenti elettronici

- **credenziali di autenticazione informatica**.
- **procedure per la gestione delle credenziali**

Athena

Il trattamento con strumenti elettronici

- Impone l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti della gestione e manutenzione degli strumenti elettronici
- Impone la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici.

Athena

Il trattamento con strumenti elettronici

- Impone che vengano effettuate delle copie di sicurezza (back up) con cadenza settimanale, che vengano adottate delle procedure per la custodia delle copie, il ripristino e la disponibilità dei dati e dei sistemi.

Athena

LO SMALTIMENTO DEI RIFIUTI TECNOLOGICI

ATTENZIONE AI DATI MEMORIZZATI IN APPARECCHIATURE ELETTRONICHE CHE ANDIAMO AD ELIMINARE….

- HARD DISK
- CHIAVI DI MEMORIA
- CD O FLOPPY DISK
- TELEFONI CELLULARI
- TABLET
- SMARTPHONE

Athena

MISURE TECNICHE OPPORTUNE

- MISURE TECNICHE PER LA MEMORIZZAZIONE DEI DATI
  - UTILIZZO DI TECNICHE DI CIFRATURA
- MISURE TECNICHE PER LA CANCELLAZIONE SICURA DEI DATI
  - USO DI APPOSITI SOFTWARE
  - DISTRUZIONE FISICA DEI SUPPORTI (sistemi di punzonatura o deformazione meccanica;distruzione fisica o di disintegrazione; demagnetizzazione ad alta intensità.)

Athena

REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

Art.30 Regolamento Ue

Athena

Soggetti obbligati alla tenuta

Titolari del trattamento

Responsabili del trattamento

- 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

Athena

Il Garante Italiano sul Registro dei trattamenti

RACCOMANDAZIONI

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.*

Contenuto del registro

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

Athena

VIOLAZIONE DATI PERSONALI

Art. 33 Regolamento UE

Athena

IL TITOLARE:

- NOTIFICA ALL'AUTORITA' 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

Athena

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

Athena

QUANDO LA VIOLAZIONE DEI DATI PERSONALI E' SUSCETTIBILE DI PRESENTARE UN **RISCHIO ELEVATO** PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

OBBLIGO DI COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI AGLI INTERESSATI

Fatta senza ritardo

Descrive in modo semplice e chiaro la natura della violazione, le possibili conseguenze, le misure adottate dal titolare

Athena

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

Athena

Valutazione di impatto sulla protezione dei dati *(PIA)*

Art.35 Regolamento UE

Athena

Obbligatoria se

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

Athena

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

Athena

La consultazione preventiva

Art.36 Regolamento UE

Athena

Quando?

- Prima di procedere al trattamento
- Se la valutazione d'impatto indica che il trattamento presenta un **rischio elevato** ed il Titolare deve quindi adottare misure idonee ad attenuare tale rischio

Athena

Contenuto della comunicazione all'Autorità di Controllo:

- Le responsabilità del titolare del trattamento, dei contitolari, dei responsabili.
- Le finalità ed i mezzi del trattamento
- Le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati
- I dati di contatto del titolare
- La valutazione d'impatto sulla protezione dei dati

Athena

procedimento:

- L'Autorità di Controllo valuta se il trattamento descritto è conforme al Regolamento e se il titolare ha identificato ed attenuato il rischio in maniera sufficiente
- In caso di esito negativo della valutazione, l'Autorità fornisce al titolare del trattamento una consulenza per iscritto

Athena

Le sanzioni

Athena

Conseguenza di una violazione

- **SANZIONI CORRETTIVE**
(avvertimenti, ammonimenti, ingiunzione di conformare i trattamenti alle norme, limitazione provvisoria o definitiva di un trattamento, ordine di rettifica cancellazione o aggiornamento)

- **SANZIONI AMMINISTRATIVE PECUNIARIE**

- **SANZIONI PENALI**

- **OBBLIGO RISARCIMENTO DANNI MORALI E MATERIALI**

Athena

Le sanzioni amministrative pecuniarie

- Determinate dal Garante

- Effettive, proporzionate e dissuasive

- Determinate tenendo conto della natura, gravità e durata della violazione, del numero di interessati lesi, del livello di danno provocato, del carattere colposo o doloso della violazione, delle misure tecniche ed organizzative messe in atto, di eventuali precedenti violazioni, del grado di cooperazione con l'Autorità

Athena

Sanzioni pecuniarie sino a 20.000.000,00 di euro euro 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

Athena

Sanzioni pecuniarie sino a 10.000.000,00 di euro euro 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

Athena

Le sanzioni penali

- Trattamento illecito di dati
- Comunicazione e diffusione illecita di dati su larga scala
- Acquisizione fraudolenta di dati su larga scala
- Falsità nelle dichiarazioni al Garante
- Inosservanza Provvedimenti del Garante
- Violazione disposizioni in materia di controlli a distanza dei lavoratori

Riepilogando….

Athena

Athena

Ricognizione dei trattamenti : cosa, chi, come e quando
(*Accountability, analisi dei rischi, azioni correttive, formazione del personale*)

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/o collaboratori)

Aggiornare le informative ed i consensi

Registri del trattamento (quando necessari)

Athena

GRAZIE DELL'ATTENZIONE