PRIVACY IN PILLOLE

ORBYTA
join the revolution

EVOLUZIONE NORMATIVA

1. DIRETTIVA EUROPEA n. 95/46/CE

L'obiettivo era quello di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

2. LEGGE n. 675/96
c.d. LEGGE SULLA PRIVACY

Riconosceva per la prima volta il diritto di chiunque alla riservatezza ed alla tutela dei propri dati personali, e fissava le "misure minime" di sicurezza necessarie per poter effettuare trattamenti di dati personali.

Abrogata dal D.Lgs n. 196/2003.

3. D.Lgs 30 giugno 2003 n. 196
c.d. CODICE DELLA PRIVACY

Un codice in materia di privacy molto vasto e ricco di allegati, che rende palese la sempre maggiore importanza della tutela del diritto alla privacy in una molteplicità di situazioni.

È diviso in tre parti: nella prima sono contenute le disposizioni generali e nella seconda alcune disposizioni specifiche, mentre nella terza trovano posto le norme relative alle forme di tutela, alle sanzioni ed all'ufficio del Garante.

4. REGOLAMENTO EUROPEO n. 2016/679 (GDPR)

Nel 2016 viene emanato il Regolamento generale sulla protezione dei dati che sostituisce la vecchia direttiva, direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio del 2018.

Per quanto riguarda l'Italia, il CODICE DELLA PRIVACY viene mantenuto sebbene sia stato profondamente modificato ed in parte abrogato dal **D.Lgs del 19 settembre 2018 n. 101.**

Le disposizioni del Codice della Privacy e del Regolamento UE 2016/679 si applicano al TRATTAMENTO DEI DATI PERSONALI…

ma cos'è un *dato personale*?

I **DATI PERSONALI** sono definiti come "*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

I dati personali vengono suddivisi in 3 categorie:

DATI IDENTIFICATIVI (o COMUNI)

dati che permettono l'identificazione diretta dell'interessato (nome e cognome, fotografia, codice fiscale, indirizzo, partita iva, e-mail, numero di polizza riferito ad un assicurato, numero di targa, codice cliente,

DATI SENSIBILI (o PARTICOLARI CATEGORIE DI DATI)

dati idonei a rivelare:

- *origine razziale ed etnica*
- *convinzioni religiose, filosofiche o di altro genere*
- *orientamento politico*
- *adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale*
- *stato di salute*

DATI GIUDIZIARI (o DATI RELATIVI A REATI E CONDANNE PENALI)

dati in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato

Il trattamento dei dati personali cd. identificativi è lecito solo se ricorre almeno una delle seguenti condizioni:

CONSENSO	L'INTERESSATO HA ESPRESSO IL CONSENSO AL TRATTAMENTO DEI PROPRI DATI PERSONALI PER UNA O PIÙ SPECIFICHE FINALITÀ
CONTRATTO	IL TRATTAMENTO È NECESSARIO ALL'ESECUZIONE DI UN CONTRATTO DI CUI L'INTERESSATO È PARTE O ALL'ESECUZIONE DI MISURE PRECONTRATTUALI ADOTTATE SU SUA RICHIESTACHIESTA DELLO STESSO;
OBBLIGO DI LEGGE	IL TRATTAMENTO È NECESSARIO PER ADEMPIERE UN OBBLIGO LEGALE AL QUALE È SOGGETTO IL TITOLARE DEL TRATTAMENTO
INTERESSE VITALE	IL TRATTAMENTO È NECESSARIO PER LA SALVAGUARDIA DEGLI INTERESSI VITALI DELL'INTERESSATO O DI UN'ALTRA PERSONA FISICA
INTERESSE PUBBLICO	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
LEGITTIMO INTERESSE	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

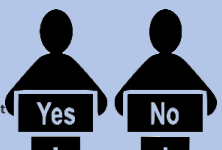
Il trattamento dei DATI PARTICOLARI (o SENSIBILI) è vietato salvo che non sussistano le seguenti condizioni di liceità:

- CONSENSO
- DIRITTO DEL LAVORO E SICUREZZA SOCIALE
- ESERCIZIO DI UN DIRITTO
- INTERESSE VITALE
- INTERESSE PUBBLICO NELLA SANITA'
- DATI RESI MANIFESTAMENTE PUBBLICI DALL'INTERESSATO
- ARCHIVIAZIONE NEL PUBBLICO INTERESSE, RICERCA SCIENTIFICA O STORICA E FINI STATISTICI
- DATI DEI MEMBRI DI UNA FONDAZIONE, ASSOCIAZIONE O ORGANISMO SENZA SCOPO DI LUCRO
- MEDICINA PREVENTIVA E DEL LAVORO, ASSISTENZA E TERAPIA SANITARIA

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

IL CONSENSO:

1. deve essere libero, specifico, informato e inequivocabile
2. il testo deve essere chiaro, semplice e comprensibile
3. non è consentito ple-flaggate le caselle online e sui testi cartacei
4. per le categorie particolari di dati il consenso deve essere esplicito
5. i minori di 18 anni non hanno diritto a dare automaticamente il proprio consenso
6. l'interessato può sempre revocare il proprio consenso
7. la revoca al consenso deve sempre essere semplice da effettuare e immediata



L'INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Prima di procedere alla raccolta (e al trattamento dei dati) è necessario fornire tutta una serie di **informazioni** all'interessati: questo è fondamentale per consentire loro di prendere decisioni informate.

Le informazioni che occorre fornire all'interessato attraverso l'informativa sul trattamento dei dati personali sono:

- **DATI DI CONTATTO DEL TITOLARE DEL TRATTAMENTO E DEL DPO**
- **FINALITA' E BASE GIURIDICA DEL TRATTAMENTO**
- **LEGITTIMI INTERESSI DEL TITOLARE O DI TERZI**
- **DESTINATARI O CATEGORIE DESTINATARI DATI PERSONALI**
- **INTENZIONE TRASFERIMENTO DEI DATI**
- **PERIODO DI CONSERVAZIONE DEI DATI**
- **DIRITTI DEGLI INTERESSATI**
- **ESISTENZA OBBLIGO LEGALE O CONTRATTUALE**
- **ESISTENZA PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)**

L'INFORMATIVA DEVE ESSERE

- concisa, trasparente, intelligibile per l'interessato e facilmente accessibile;
- chiara e semplice;
- in linea di principio, per iscritto e preferibilmente in formato elettronico;

TEMPI DELL'INFORMATIVA

- Se i dati sono raccolti direttamente presso l'interessato: deve essere fornita all'interessato prima di effettuare la raccolta dei dati.

- Se i dati non sono raccolti direttamente presso l'interessato: l'informativa deve essere fornita entro un termine ragionevole che non può comunque superare 1 mese dalla raccolta, oppure al momento della comunicazione dei dati.

I SOGGETTI DEL TRATTAMENTO DEI DATI PERSONALI

IL TITOLARE

È la persona fisica, persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza

IL RESPONSABILE

Quando un trattamento viene effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE e garantisca la tutela dei diritti dell'interessato. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico.

IL *DATA PROTECTION OFFICER* DPO

Ha il compito di:

- informare il titolare o il responsabile del trattamento in merito agli obblighi derivanti dal Regolamento, delle altre disposizioni dell'UE o degli Stati membri;
- verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
- fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
- fungere da punto di contatto per il Garante per la protezione dei dati personali oppure,

INCARICATO o AUTORIZZATO

soggetto che svolge le operazioni di trattamento sotto la diretta autorità del titolare, attenendosi alle istruzioni da quest'ultimo impartite.

Per svolgere tali operazioni, l'incaricato deve essere espressamente autorizzato al trattamento dei dati.

L'incaricato al trattamento deve sempre:

- svolgere le operazioni di trattamento in relazione alle mansioni spettanti in esecuzione della prestazione lavorativa, e potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati.
- verificare, prima del trattamento stesso, che sia stata resa all'interessato l'informativa sul trattamento dei dati personali;
- richiedere e utilizzare esclusivamente i dati necessari alla normale attività lavorativa;
- custodire i dati oggetto del trattamento in luoghi non accessibili a non autorizzati;
- non lasciare incustodita e accessibile a terzi la propria postazione di lavoro e prima di aver provveduto alla messa in sicurezza dei dati, evitando così che vengano consultati e/o prelevati da persone prive di autorizzazione;
- non lasciare incustodito e accessibile a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni di consultazione;
- assicurare la segretezza delle credenziali;
- mantenere la massima riservatezza sui dati trattati e non comunicare i dati a soggetti non autorizzati;
- osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali;
- osservare le istruzioni impartite dal Titolare mediante il codice disciplinare interno e le procedure.

MISURE DI SICUREZZA

Tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza e la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio.

Le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

Sicurezza dei dati significa anche non divulgare i dati con troppa leggerezza…

E' pertanto fondamentale che si presti attenzione a:

- quali dati si condividono;
- con chi si condividono i dati;
- ricordarsi di rimuovere dalle liste di autorizzazione chi non ha più diritto di accedere a determinati dati;
- non comunicare MAI ad altri le proprie credenziali, neppure ai propri colleghi;
- salvare i dati aziendali su fileserver o cloud.

INCIDENTI DI SICUREZZA

Un incidente di sicurezza (o *data breach*) è un vero e proprio imprevisto (*incident*) che colpisce l'utente o l'azienda mettendo a rischio la segretezza e riservatezza del dato.

Alcuni esempi:

- **DEVICE INFETTO**: un pc infetto con un *logger* o un *tracker* può mettere in serio pericolo l'azienda poiché potrebbe raccogliere password per autorizzare accessi ad aree sensibili;
- **SMARRIMENTO/FURTO DI UN DEVICE**: un device non adeguatamente protetto, potrebbe permettere l'accesso ai dati aziendali da parte di terzi non autorizzati;
- **FURTO/HACKING DI CREDENZIALI**: oltre che essere ovviamente un danno, rende anche difficile l'identificazione di chi abbia effettivamente avuto accesso al dato;
- **VULNERABILITÀ**: sistemi non aggiornati potrebbero dare spazio a backdoor.

COME EVITARLI?

- **cambiare spesso la password**

- **collegarsi in VPN o alla rete aziendale** in modo tale da permettere al vostro pc di aggiornare le policy così da aumentare la sicurezza del device

- **riavviare il pc dopo gli aggiornamenti** almeno una volta alla settimana, questo permetterà l'installazione degli aggiornamenti

- **prestare attenzione a mail, allegati & software**: molti software sono gratuiti e sembrano affidabili, tanto quanto alcune mail. Fare quindi attenzione alla fonte e all'attendibilità del contenuto.

CREDENZIALI DI AUTENTICAZIONE

L'accesso al sistema operativo del PC, alla mail e ad eventuali software gestionali utilizzati nonché agli altri strumenti elettronici, deve avvenire tramite l'utilizzo delle "**credenziali di autenticazione** (es. "Username" e "Password"

- Le credenziali di autenticazione costituiscono dati dell'organizzazione da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi.
- Ognuno è responsabile dell'utilizzo del proprio account Utente. Se si ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è necessario modificare

La **PASSWORD**:

- deve essere composta da almeno 8 caratteri, deve essere alfanumerica e, possibilmente, contenere almeno un carattere speciale;
- non deve contenere riferimenti facilmente riconducibili all'incaricato;
- va modificata sempre al primo accesso e, almeno ogni 6 mesi (3 mesi nel caso di trattamento di dati particolari o giudiziari) o immediatamente nei casi in cui sia compromessa (anche nel caso vi sia il sospetto);
- deve essere sempre mantenuta riservata: pertanto no va trascritta su supporti facilmente accessibili a terzi (es. fogli, post-it), né va lasciata memorizzata sul proprio PC.

PHISHING

Il c.d. phishing consiste in una truffa realizzata attraverso l'inganno degli utenti.
Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli provenienti da mittenti **apparentemente** conosciuti o noti.

Il messaggio invita l'utente - solitamente riferendo problemi di registrazione o di altra natura - a fornire i propri dati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web in questione o del servizio a cui si è registrati.

I messaggi di posta elettronica possono contenere anche virus.
La modalità più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf.

Per questo è importante prestare sempre attenzione al mittente e al contenuto del messaggio e proteggere il PC con degli **antivirus** sempre aggiornati.

ANTIVIRUS

I Malware e i Virus sfruttano vulnerabilità intrinseche del software, al fine di alterare e utilizzare in maniera illegittima le risorse del sistema che lo ospita…

Come prevenirli e rimuoverli:

- I PC devono essere dotati di programmi antivirus aggiornati all'ultima versione disponibile;
- non utilizzare programmi non attendibili scaricati da Internet;
- Non aprire mai mail inattese o comunque di provenienza o contenuto incerti;
- Non cliccare su link contenuti all'interno di mail di cui non sia assolutamente certa la provenienza.

A volte prestare attenzione potrebbe non essere sufficiente…

Se si verifica un incidente di sicurezza o un malfunzionamento del PC in generale, occorre avvisare immediatamente il Titolare del trattamento.

Contattare, non appena possibile, anche il Supporto IT all'indirizzo help@orbyta.it.

TRASMISSIONE DEI DOCUMENTI

Quando i dati personali devono essere inviati a mezzo fax, posta elettronica, ecc. occorre:

- prestare la massima attenzione affinché l'indirizzo e-mail del destinatario immesso sia corretto;
- accertarsi sempre che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare, verificando sempre che i documenti in allegato siano quelli di cui il destinatario abbia titolo per prenderne visione.
- nel caso in cui si debba procedere all'invio tramite posta elettronica di informazioni altamente riservate, o documenti contenenti dati sensibili (cd. "particolari categorie di dati") è necessario crittografare o criptare il file contenente tali dati, ovverosia proteggerlo con una password;

FOTO E VIDEO

PRIMA di procedere alla registrazione di video o di fotografie nonché prima di procedere alla loro pubblicazione e/o diffusione è necessario accertarsi che l'interessato abbia preso visione dell'informativa sul trattamento dei dati personali e abbia espressamente prestato il proprio consenso per iscritto.

In mancanza, sarà necessario astenersi dal porre in essere tali azioni.

DOCUMENTI CARTACEI

i documenti cartacei contenti dati personali devono essere conservati in archivi muniti di serratura e collocati in uffici con accesso riservato ai soli soggetti incaricati o autorizzati.

possono accedere alle informazioni contenute nell'archivio cartaceo solo i soggetti autorizzati

i documenti cartacei contenenti dati personali non devono mai essere lasciati incustoditi o comunque in luogo accessibile a soggetti non autorizzati

FOTOCOPIATRICI E STAMPANTI

L'utilizzo di copie fotostatiche deve essere limitato e avvenire solo quando sia strettamente necessario.

Al fine di evitare che persone non autorizzate possano venire a conoscenza di informazioni riservate o accedere a dati personali al cui trattamento non sono state autorizzate, è opportuno ritirare immediatamente le copie non appena inviate in stampa, evitando in questo modo di lasciare le stampe incustodite.

Non è consentito utilizzare carta da recupero recante, sul retro, dati personali.

Prima di gettare un documento è preventivamente opportuno procedere alla sua distruzione mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo (anche strappando i fogli manualmente) che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

SANZIONI

In caso di violazione delle regole che disciplinano il trattamento dei dati ci può essere una responsabilità del titolare o del responsabile:

RESPONSABILITÀ CIVILE

Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

RESPONSABILITÀ AMMINISTRATIVA

Il Regolamento UE 2016/679 stabilisce che la violazione delle disposizioni in materia di protezione dei dati personali è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000,00 euro, o per le imprese, fino al 4 % del fatturato totale annuo.

RESPONSABILITÀ PENALE

comporta l'applicazione di pene detentive o pecuniarie da parte dell'Autorità Giudiziaria (**sanzioni penali**)

a titolo esemplificativo…

L'art. 167 del Codice sulla privacy punisce chi al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, arreca nocumento all'interessato in violazione di specifiche disposizioni di legge.

L'art. 167-bis del Codice sulla privacy punisce la comunicazione e la diffusione di dati personali oggetto di trattamento su larga scala, al fine di trarre profitto ovvero al fine di arrecare danno.

L'art. 167-ter del Codice sulla privacy prevede il reato di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.

Documento redatto da ORBYTA LEGAL