

CODICE SULLA PRIVACY

GLOSSARIO

1 - ACCERTAMENTI

Il Garante può disporre accessi a banche dati, archivi o altre ispezioni e verifiche nei luoghi dove si svolge il trattamento o dove occorre effettuare rilevazioni utili al controllo del rispetto della normativa sulla privacy.

2 - ACCESSO

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se ancora non registrati e la loro comunicazione in forma intelligibile.

3 - AUTENTIFICAZIONE INFORMATICA

Insieme degli strumenti elettronici e delle procedure per la verifica dell'identità.

4 - AUTORIZZAZIONE

Provvedimento adottato dal Garante con il quale il titolare (azienda, ente e libero professionista) viene autorizzato a trattare dati sensibili o giudiziari o a trasferire dati all'estero. Sette autorizzazioni generali adottate dall'Authority consentono trattamenti per scopi specifici (es.: rapporti di lavoro, sondaggi e ricerche, attività di selezione del personale), senza che sia necessario presentare al Garante una richiesta di autorizzazione.

5 - BANCA DATI

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità, dislocate in uno o più siti.

6 - BLOCCO

Conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

7 - CANCELLAZIONE

Diritto di ottenere l'eliminazione di dati per i quali è venuta meno la necessità di effettuare il trattamento. Non è possibile ottenere la distruzione o l'alterazione del documento se perdura l'obbligo legale di conservarlo.

8 - CESSAZIONE DEL TRATTAMENTO

In caso di cessazione di un trattamento i dati possono essere distrutti, ceduti ad altro titolare a condizione che siano destinati a un trattamento compatibile agli scopi per i quali sono raccolti. Possono essere conservati per fini personali ma non usati per comunicazioni o diffusi, oppure possono essere conservati per

scopi storici, statistici o scientifici rimanendo nell'ambito della legge, dei regolamenti, della normativa comunitaria e dei codici di deontologia e di buona condotta.

9- CODICI DI DEONTOLOGIA

il Codice della privacy rafforza l'importanza dei codici deontologici e di buona condotta prevedendone la sottoscrizione in molteplici settori (es: trattamenti delle "centrali rischi" private, delle attività investigative, per scopi statistici ecc).

10 - COMUNICAZIONE

Far conoscere dati personali a uno o più soggetti diversi dall'interessato, dal responsabile e dagli incaricati in qualsiasi forma anche rendendoli disponibili o consultabili.

11 - CONSENSO

Qualsiasi trattamento di dati personali da parte di privati o di enti pubblici economici può essere effettuato solo con il consenso dichiarato dall'interessato, preventivamente informato da chi gestisce i dati. Il consenso deve essere manifestato liberamente e specificatamente in riferimento a un trattamento chiaramente individuato. Deve essere annotato dal titolare, dal responsabile o da un incaricato del trattamento su un registro o su un verbale. Può riguardare l'intero trattamento o una o più operazioni. Se i dati sono sensibili deve essere dato per iscritto.

12 – CONTROLLO A DISTANZA

il Codice ribadisce il divieto di controllo a distanza dei lavoratori. In base allo Statuto dei lavoratori impianti e apparecchiature di controllo richiesti da esigenze organizzative, produttive o di sicurezza sul lavoro dai quali derivi anche la possibilità di controllo dei lavoratori possono essere installati solo previo accordo con le rappresentanze sindacali aziendali o, in mancanza, con la commissione interna. In difetto di accordo spetta all'Ispektorato del lavoro, su richiesta del datore, dettare le modalità di uso degli impianti di controllo.

13 – CREDENZIALI DI AUTENTIFICAZIONE

Dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

1 – DATI GIUDIZIARI

Sono quei dati idonei a rilevare l'esistenza di provvedimenti giudiziari penali soggetti ad iscrizione nel casellario giudiziario (condanne definitive, libertà condizionale, divieto o obbligo di soggiorno, misure alternative alla detenzione), delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato e di indagato ai sensi del codice di procedura penale.

14 - DATI IDENTIFICATIVI

Sono i dati personali che permettono l'identificazione diretta dell'interessato (es: nome, un numero di riconoscimento...).

15 – DATI SENSIBILI

Sono quei dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Sono dati sensibili ad esempio le trattenute sindacali, i dati relativi ad infortuni o malattie, i dati delle cartelle cliniche, radiografie ecc.

16 – DATO ANONIMO

Dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.

17 – DATO PERSONALE

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Sono, pertanto, dati personali ad esempio: i dati anagrafici, il codice fiscale, il domicilio, il numero di telefono...).

18 - DIFFUSIONE

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

19 – DOCUMENTO PROGRAMMATICO SULLA SICUREZZA - DPS

Misura minima che deve essere adottata dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici.

Il Documento programmatico sulla sicurezza deve indicare:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

20 - FIREWALL

Strumento elettronico per garantire la sicurezza delle reti aziendali.

21 - GARANTE

E' un'autorità amministrativa indipendente che ha il compito di vigilare sul rispetto delle norme di protezione dei dati personali. Si compone di quattro membri eletti dal Parlamento.

Esamina reclami e segnalazioni dei cittadini e vigila sulle norme di tutela della vita privata. Decide sui ricorsi dei cittadini, emette pareri, compie ispezioni, vieta trattamenti illeciti di dati, commina sanzioni amministrative pecuniarie, informa l'autorità giudiziaria in caso di gravi illeciti.

22 - HANDICAP

Il Codice della privacy ha introdotto una specifica norma relativa ai contrassegni rilasciati a persone invalide: devono essere esposti sui veicoli e contenere solo i dati indispensabili a individuare l'autorizzazione rilasciata, senza apposizione di simboli e diciture. Generalità e indirizzo della persona fisica interessata non devono essere direttamente visibili sul contrassegno.

23 - INCARICATI

Persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

24 - INFORMATIVA

L'interessato deve essere informato preventivamente, oralmente o per iscritto, relativamente a:

- finalità e modalità del trattamento;
- indicazioni riguardo la natura obbligatoria o facoltativa del conferimento dei dati e conseguenze dell'eventuale rifiuto;
- soggetti e categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza;
- i diritti dell'interessato;
- i dati del titolare del trattamento e se nominato del responsabile.

25 - INTERESSATO

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

26 - INTERPELLO PREVENTIVO

Il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile del trattamento, se sono decorsi i termini (15 giorni dal ricevimento senza riscontri, 30 giorni per un integrale riscontro alla richiesta) o si è ottenuto un diniego, anche parziale.

27 - INTRUSIONE DETECTION SYSTEM

Strumenti che permettono di analizzare e verificare le attività in corso sulla rete e sui sistemi con lo scopo di individuare eventuali segnali di pericolo.

28 - LAVORO

Nell'ambito lavorativo è vietato il controllo a distanza dei lavoratori.
Sono previste particolari garanzie nei casi in cui le telecamere devono essere installate per esigenze organizzative e dei processi produttivi o sono richieste da esigenze legate alla sicurezza del lavoro.
Inammissibili le telecamere in luoghi non destinati ad attività lavorativa come bagni, spogliatoi, docce, armadietti e luoghi ricreativi.

29 – LUOGHI DI CURA

Amnesso il monitoraggio dei pazienti ricoverati in particolari reparti come, ad esempio, la rianimazione.
Alle immagini possono accedere personale autorizzato e familiari dei ricoverati in reparti dove non sia consentito recarsi personalmente.

30 - MINORI

E' vietato pubblicare e divulgare con qualsiasi mezzo notizie o immagini idonee a identificare minori, anche in caso di coinvolgimento del bambino in procedimenti giudiziari anche non di natura penale.

31 – MISURE DI SICUREZZA

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, i rischi di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito. In taluni casi (ad es. per i fornitori di servizi di comunicazione) servono speciali cautele essendo anche necessario informare gli abbonati oppure gli utenti dell'esistenza di determinati rischi oltre che di rimedi e relativi costi.

32 – MISURE MINIME

Complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza obbligatorie volte ad assicurare un livello minimo di protezione ai dati personali.

33 - NOTIFICAZIONE

Comunicazione al Garante, una volta sola ed esclusivamente per via telematica, di determinate tipologie di utilizzo dei dati, in gran parte sensibili.
L'obbligo di notificazione è diventato più snello e l'Autorità ha individuato numerosi casi di esonero.

34 – OPT / IN

Per trattare qualunque informazione personale è necessario ricevere il consenso preventivo dell'interessato. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

35 – OPT / OUT

Rifiuto a posteriori dell'utente a ricevere messaggi indesiderati.

36 – PAROLA CHIAVE

Componente di una credenziale di autenticazione associata a una persona e a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

37 – PROFILO AUTORIZZAZIONE

Insieme delle informazioni, univocamente associate a una persona, che consente di individuare a quali dati può accedere e i trattamenti consentiti.

38 - QUESITI

E' possibile inviare al Garante dei quesiti o delle richieste di informazioni contattando l'ufficio relazioni con il pubblico di Piazza Monte Citorio 121, 00186 Roma.

L'ufficio risponde dal lunedì al venerdì dalle 10 alle 13, telefonando al n. 06.696.77.917 o inviando una e-mail a urp@garanteprivacy.it

39 - RECLAMO

Si può proporre al Garante un reclamo circostanziato per rappresentare una violazione della disciplina in materia di trattamento dei dati personali. Il reclamo è sottoscritto agli interessati o da associazioni che li rappresentano ed è presentato al Garante senza particolari formalità.

40 – RESPONSABILE DEL TRATTAMENTO

E' la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

41 – RETE DI COMUNICAZIONE

Sistemi di trasmissione, apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, tramite radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici.

Sono incluse le reti satellitari, terrestri mobili e fisse a commutazione di circuito e di pacchetto, compresa internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

42 – RETE PUBBLICA DI COMUNICAZIONE

Rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico.

43 - RETTIFICA

Diritto di ottenere la correzione di dati personali inesatti.

44 - RICORSO

I diritti di accesso, aggiornamento, rettifica e cancellazione dei dati personali possono essere fatti valere con ricorso al Garante, che non può essere proposto se è stata già adita l'Autorità Giudiziaria.

45 – SCREENING ROUTER

Strumento elettronico che intercetta, nasconde e respinge i pacchetti di dati che rispondono a certe caratteristiche e che potrebbe rivelarsi un attacco ostile.

46 – SISTEMA DI AUTORIZZAZIONE

Insieme di strumenti e procedure che abilitano l'accesso ai dati e alle modalità di trattamento, in funzione del profilo di autorizzazione del richiedente.

47 – SMART CARD

Credenziale di autenticazione consistente in un dispositivo che somiglia a una comune carta di credito nel quale è inserito un microprocessore dotato di una memoria per la registrazione di una certa quantità di dati.

48 - SPAMMING

Inoltro di messaggi di posta elettronica non sollecitati, aventi carattere pubblicitario o commerciale. Il Garante ha adottato il provvedimento 29 maggio 2003 relativo alla pratica di invio di messaggi indesiderati.

49 – STRUMENTI ELETTRONICI

Elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

50 – TECNOLOGIE BIOMETRICHE

Sistemi con cui si identificano le persone in base ad alcune caratteristiche fisiche: impronte digitali, iride, retina, volto, Dna.

51 – TITOLARE DEL TRATTAMENTO

Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche insieme ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

52 – TRASFERIMENTO DEI DATI ALL'ESTERNO

I flussi di dati verso un Paese situato oltre i confini dell'Unione Europea sono consentiti solo se quello Stato assicura un adeguato livello di tutela delle persone o se sussiste uno dei presupposti di liceità indicati dalla normativa nazionale (consenso dell'interessato, adempimento degli obblighi contrattuali).

53 – TRASPORTO URBANO

L'installazione sui mezzi pubblici di trasporto o alle fermate è lecita in situazioni di particolare rischio, legate a fenomeni di criminalità come aggressioni e borseggi.

Occorre particolare cura per l'angolo visuale delle riprese (evitando particolari non rilevanti dei passeggeri) e nella collocazione di informative a bordo dei mezzi e delle fermate.

54 - TRATTAMENTO

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'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione, la distruzione di dati, anche se non registrati in una banca dati.

55 - UTENTE

Qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

56 – VIDEOCITOFONI

Insieme agli apparecchi che rilevano immagini o suoni senza registrazione sono ammissibili per identificare chi entra in luoghi privati.

La loro esistenza deve essere resa nota tramite un’informativa agevolmente rilevabile, quando non sono utilizzati per fini strettamente personali.

57 – VIDEOSORVEGLIANZA

Trattamento di dati personali effettuato con strumenti elettronici di rilevamento di immagini.

L’installazione di telecamere è lecita solo se è proporzionata agli scopi che si intendono perseguire: gli impianti devono essere attivati solo quando altre misure (sistemi di allarme, controlli fisici e logistici, misure di protezione degli ingressi) siano realmente insufficienti o inattuabili. L’eventuale conservazione di immagini deve essere limitata nel tempo.

Il cittadino deve sempre essere informato sul fatto che sta per accedere in una zona videosorvegliata. L’informativa, in formato chiaramente visibile, deve indicare con formula sintetica la presenza di telecamere. Può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione. L’uso illecito di sistemi di videosorveglianza espone a provvedimenti di blocco, sanzioni amministrative e penali.

58 - ZTL

Per i contrassegni di accesso alle zone a traffico limitato dei centri storici il Codice della Privacy ha introdotto una specifica norma: devono essere esposti sui veicoli e contenere solo i dati indispensabili a individuare l’autorizzazione rilasciata, senza apposizione di simboli e diciture.

Generalità e indirizzo della persona fisica interessata non devono essere direttamente visibili sul contrassegno.

Per introdurre sistemi di rilevazione degli accessi dei veicoli ai centri storici e a traffico limitato i Comuni devono chiedere una specifica autorizzazione amministrativa e limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione.

I dati possono essere conservati solo per il periodo necessario a contestare infrazioni e a definire il relativo contenzioso.

Si può accedere a questi dati solo a fini di polizia giudiziaria o di indagine penale.