

Accorgimenti

PER LA SICUREZZA ED IL CORRETTO TRATTAMENTO DEI
DATI PERSONALI

TRATTAMENTO DEI DATI NELLE PUBBLICHE AMMINISTRAZIONI

- **il trattamento dei dati sensibili e giudiziari** se autorizzato da espressa disposizione di legge nella quale si specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, le amministrazioni sono tenute ad adottare un apposito regolamento con il quale identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dal Codice.

In ogni caso, il trattamento dei dati sensibili e giudiziari da parte delle Pubbliche Amministrazioni è retto dal principio di indispensabilità, ossia possono essere trattati soltanto i dati sensibili e giudiziari indispensabili allo svolgimento di funzioni istituzionali che non potrebbero essere adempiute altrimenti (mediante il ricorso a dati anonimi o personali di diversa natura).

la comunicazione di dati personali

- a privati o enti pubblici economici soltanto se prevista da una norma di legge o di regolamento
- ad altri soggetti pubblici se prevista da una norma di legge o di regolamento ovvero, in mancanza, se necessaria per il perseguimento dei fini istituzionali previa apposita comunicazione al Garante per la protezione dei dati personali.

Non è in ogni caso consentita la diffusione dei dati idonei a rilevare lo stato di salute.

Misure di sicurezza da adottare vengono distinte in:

- **misure idonee e preventive** volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- **misure minime**, indicate negli articoli 34 e 35 e analiticamente specificate nel Disciplinare Tecnico e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici.

Con l'approvazione del Codice i titolari di trattamento di dati sono tenuti ad adottare, quanto meno, le cd "misure minime di sicurezza", ossia gli accorgimenti, individuati negli artt. 34-35 e nel Disciplinare Tecnico del Codice, tesi ad assicurare un livello minimo di protezione dei dati personali.

La mancata osservanza di quanto stabilito in materia di misure minime di sicurezza è sanzionata penalmente

L'adozione delle misure minime di sicurezza non esonera tuttavia da responsabilità civile qualora l'eventuale danneggiato dimostri che, in base all'evoluzione tecnologica raggiunta, era possibile e raccomandabile l'utilizzo di misure di sicurezza ulteriori (le cd misure "idonee").

PRECAUZIONI GENERALI DA ADOTTARE NEL TRATTAMENTO DI DATI PERSONALI CONTENUTI IN ARCHIVI E DOCUMENTI CARTACEI

Trattamento di documenti contenenti dati personali

1. Gli incaricati sono tenuti a custodire e controllare gli atti e i documenti contenenti dati personali, in modo da evitare che persone prive di autorizzazione possano accedere ai dati.
2. I documenti contenenti dati personali devono essere conservati in archivi ad accesso controllato e con possibilità di chiusura, solo il personale autorizzato, secondo le modalità specificate nella lettera d'incarico, avrà la possibilità di averne accesso.
3. Tutta la documentazione e le pratiche trattate o da trattare devono essere riposte in armadi chiusi a chiave nel periodo di intervallo meridiano o al termine della giornata lavorativa.
4. La protezione dei dati deve essere compiuta dalla loro acquisizione fino all'eventuale distruzione degli stessi e per tutto il ciclo di loro trattamento e conservazione.
5. Gli incaricati **devono** evitare che terzi (non incaricati), possano accedere ai luoghi in cui sono custoditi i dati, quindi devono adottare misure idonee per evitare la visibilità dei dati a terzi.
6. Non è possibile effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile della **sicurezza dei dati personali** di dati oggetto del trattamento.
7. Non è possibile effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
8. Non è possibile sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
9. Sarà cura di ogni incaricato adottare ogni misura possibile al fine di garantire quanto sopra.

LE MISURE MINIME DI SICUREZZA

Trattamenti effettuati con strumenti elettronici TRATTAMENTO DATI COMUNI

Sono obbligatorie le seguenti misure:

A) AUTENTICAZIONE INFORMATICA.

Il sistema informatico deve essere dotato di mezzi (le cd. credenziali di autenticazione) deputati alla verifica ed alla convalidazione dell'identità del soggetto che vi accede. Le credenziali di autenticazione consistono in un codice per l'identificazione (user id) dell'incaricato associato a una parola chiave riservata (password), conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

B) ADOZIONE DI PROCEDURE DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE;

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri

oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali

C) UTILIZZAZIONE DI UN SISTEMA DI AUTORIZZAZIONE;

E' il sistema che, dopo l'autenticazione, permette agli incaricati di trattare effettivamente i dati.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione

D) AGGIORNAMENTO PERIODICO DELL'INDIVIDUAZIONE DELL'AMBITO DEL TRATTAMENTO CONSENTITO AI SINGOLI INCARICATI E ADDETTI ALLA GESTIONE O ALLA MANUTENZIONE DEGLI STRUMENTI ELETTRONICI;

E' effettuata tramite l'aggiornamento, almeno annuale, dell'anagrafe del trattamento dei dati personali.

E) PROTEZIONE DEGLI STRUMENTI ELETTRONICI E DEI DATI RISPETTO A TRATTAMENTI ILLECITI DI DATI, AD ACCESSI NON CONSENTITI E A DETERMINATI PROGRAMMI INFORMATICI;

Utilizzo di antivirus aggiornati almeno semestralmente (giornalmente) e adozione di misure atte alla protezione dagli accessi dalla rete (firewall etc)

F) ADOZIONE DI PROCEDURE PER LA CUSTODIA DI COPIE DI SICUREZZA, IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI E DEI SISTEMI;

Utilizzo di back up e strategie di disaster recovery

TRATTAMENTO DATI SENSIBILI O GIUDIZIARI

Ulteriori misure:

H) ADOZIONE DI IDONEE MISURE PER GARANTIRE IL RIPRISTINO DELL'ACCESSO AI DATI IN CASO DI DANNEGGIAMENTO DEGLI STESSI O DEGLI STRUMENTI ELETTRONICI, IN TEMPI CERTI COMPATIBILI CON I DIRITTI DEGLI INTERESSATI E NON SUPERIORI A SETTE GIORNI

i) Devono essere concordate con il titolare del trattamento o gli amministratori di sistema le misure organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati

sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (DATI SU SUPPORTO CARTACEO)

Trattamento dati comuni

Sono **obbligatorie** le seguenti misure:

- a) L'aggiornamento periodico dei dati il cui trattamento è consentito agli incaricati (tramite l'aggiornamento dell'anagrafe dei trattamenti)
- b) Istruzioni circa un'idonea custodia degli atti e dei documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

E' compito di ciascun responsabile fornire istruzioni agli incaricati del trattamento affinché ai documenti contenenti dati personali non accedano persone prive di autorizzazione, dando idonea divulgazione presso gli stessi del presente Manuale per la sicurezza, per quanto riguarda le prescrizioni di carattere generale, nonché impartendo le istruzioni del caso relativamente alla specificità del trattamento dei dati personali effettuato nell'Unità Organizzativa medesima.

TRATTAMENTO DATI SENSIBILI O GIUDIZIARI

Ulteriori misure:

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, possibilmente utilizzando armadi o contenitori chiusi a chiave. Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

1. Tali dati dovranno essere custoditi in appositi armadi muniti di serratura, solo in personale specificatamente autorizzato preposto al trattamento di questi dati, secondo le modalità specificate nella lettera d'incarico, avrà la possibilità di averne accesso. Tali armadi dovranno sempre rimanere chiusi, e solo il personale o l'incaricato potrà avere la chiave per poter effettuare l'apertura degli stessi. È assolutamente **VIETATO** lasciare incustodito e aperti, anche solo temporaneamente tali archivi;

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

1. UTILIZZATE LE CHIAVI!

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio quando l'ultima unità di personale lascia il locale e, comunque, alla fine della giornata e chiudete i documenti a chiave negli armadi ogni volta che potete.

2. NON COMUNICATE DATI PERSONALI A SOGGETTI NON LEGITTIMATI

L'utilizzo dei dati personali deve avvenire in base al cd "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi, se non previa autorizzazione del Responsabile nelle ipotesi consentite dalla normativa vigente.

3. FATE ATTENZIONE A COME DISTRUGGETE I DOCUMENTI

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

4. RADDOPPIATE LE ATTENZIONI SE I DOCUMENTI CONTENGONO DATI SENSIBILI O GIUDIZIARI

I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione.

Ad esempio, la consultazione di documenti o certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattia, ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave. Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

Riponete i documenti contenenti dati sensibili o giudiziari negli appositi contenitori o arma al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

Particolare attenzione dovrà essere rivolta ai documenti contenenti dati sensibili o giudiziari con particolare attenzione alla documentazione sanitaria contenuta nelle schede. A tal fine è necessario che tali documenti, quando sono al di fuori dei loro archivi durante l'utilizzo quotidiano, siano tenuti sotto il controllo e la custodia degli incaricati, mentre al termine dell'impiego quotidiano, devono essere riposti in armadi, cassetti, archivi o contenitori chiusi a chiave. Non devono assolutamente essere lasciati sulle scrivanie o postazioni di lavoro a disposizione di chiunque entri nell'ufficio/locale. In caso di ingresso nel locale/ufficio di persone estranee è buona norma fare in modo di impedire l'accesso a tali documenti, ad esempio conservandoli temporaneamente in un cassetto o in una teca, sempre comunque sotto il controllo dell'incaricato. Si ricorda inoltre, di provvedere alla separazione dei dati sensibili (idonei a rilevare lo stato di salute e vita sessuale, da altri dati non necessari alle finalità del trattamento). Ad esempio, i certificati medici possono essere mantenuti nel faldone contenente la documentazione dell'interessato ma separandoli dagli altri documenti, ad esempio, utilizzando una busta chiusa.

TRATTAMENTI CON STRUMENTI ELETTRONICI

1. CONSERVATE I DATI IN UN LUOGO SICURO

Si applicano gli stessi criteri che per i documenti cartacei. Riponeteli negli armadi o nei cassetti non appena avete finito di usarli.

2. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- a) La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
- b) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
- c) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.

- d) La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.
- e) Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, esclusivamente ai tecnici accreditati incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

3. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe.

4. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i furti. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

5. NON FATEVI SBIRCIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattilo-scrittura.

6. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

7. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata.

8. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con responsabile/amministratore di sistema.

9. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME NON SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

Guida ai primi accorgimenti per il Nuovo Regolamento Europeo 679/2016.

Principali accorgimenti utili all'immediata applicazione del nuovo Regolamento Ue.

Fonti: Rete – Garante Privacy – Agi – legaldesk.

Il GDPR si basa, infatti, sul principio di "responsabilizzazione" (in inglese accountability) di chiunque effettui operazioni di trattamento nell'ambito della propria attività (il cosiddetto "titolare del trattamento"). Significa, quindi, che ciascuno dovrà fare le valutazioni e le scelte adatte alla propria specifica realtà. E le sanzioni per l'inosservanza delle norme possono arrivare fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale. Particolare attenzione è dedicata alla tutela dei minori che - per accedere ai servizi della società dell'informazione (come i social network) - devono avere almeno 16 anni per poter prestare autonomamente il consenso al trattamento.

Il Regolamento è destinato ad abrogare la Direttiva 95/46 che ha portato l'Italia all'adozione dell'attuale Codice Privacy (il Decreto Legislativo n. 196/2003)

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'ideale base giuridica. Particolarmente:

1) Gli obblighi nei confronti degli utenti

Gli utenti devono essere informati in modo semplice e chiaro sulle finalità, modalità e ambito del trattamento. Le informative richieste agli utenti (dal form per una newsletter ai moduli per richiedere una fidelity card) devono quindi essere aggiornate, prevedendo alcune informazioni nuove (come la base giuridica del trattamento e il tempo di conservazione dei dati) e semplificando il testo in modo da renderle realmente comprensibili.

2) Le misure tecniche da adoperare

Ogni titolare del trattamento è tenuto ad adottare misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati. Non esiste un elenco di misure di sicurezza "minime" uguali per tutti. Spetta a ciascuno decidere e assumersi le responsabilità di quali siano le contromisure adeguate alla propria realtà (crittografia, controllo degli accessi, sorveglianza degli archivi, ecc.).

3) Viene introdotto il diritto degli interessati di venire a conoscenza delle violazioni dei propri dati personali ("data breach"). Questo significa che - nel caso di incidenti di sicurezza relativi ai sistemi utilizzati per il trattamento (come lo smarrimento di una chiavetta Usb, il furto di un fascicolo oppure un attacco informatico) - il titolare del trattamento dovrà organizzarsi per procedere alla notificazione al Garante Privacy senza ritardo (e comunque, entro le 72 ore).

4) Le sanzioni

Il sistema sanzionatorio previsto del GDPR è molto più severo rispetto a quello del Codice Privacy. Le sanzioni amministrative - che saranno inflitte dal Garante Privacy - possono arrivare fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale. Le sanzioni non sono però l'unico spauracchio. In attesa di vedere se e quali saranno gli illeciti penalmente rilevanti previsti dal Decreto che il governo italiano si appresta ad adottare, è importante tenere a mente che chiunque subisca un danno da una violazione del GDPR ha il diritto di ottenerne il risarcimento dal titolare, a meno che quest'ultimo non dimostri che il danno non gli è alcun modo imputabile. E forse questa è alla fine la prova più difficile da dare se non sono state affrontate tutte le novità del GDPR.

QUINDI

IL CONSENSO



COSA
CAMBIA

- Per i dati “sensibili” (si veda art. 9 regolamento) il consenso deve essere “esplicito”; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).
Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo “Articolo 29” (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.
- Non deve essere necessariamente “documentato per iscritto”, né è richiesta la “forma scritta”, anche se questa è modalità idonea a configurare l’inequivocabilità del consenso e il suo essere “esplicito” (per i dati sensibili); inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l’interessato ha prestato il consenso a uno specifico trattamento.

Contenuti dell’informativa



COSA
CAMBIA

- I contenuti dell’informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest’ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).
- Il regolamento prevede anche ulteriori informazioni in quanto “necessarie per garantire un trattamento corretto e trasparente”: in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all’autorità di controllo.
- Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l’informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l’interessato.

Tempi dell’informativa



COSA
CAMBIA

- Nel caso di dati personali non raccolti direttamente presso l’interessato (art. 14 del regolamento), l’informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all’interessato) (diversamente da quanto prevede attualmente l’art. 13, comma 4, del Codice).

Modalità dell'informativa



- Il regolamento specificò molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
- L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'UE e saranno definite e prossimamente dalla Commissione europea.
- Sono inoltre parzialmente diversi i requisiti che il regolamento fissò per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che spetta al titolare.

Registro dei trattamenti

- Tutti i titolari e i responsabili di trattamento devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Notifica delle violazioni di dati personali

- A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della

comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento. Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo “Articolo 29”, qui disponibili: www.garanteprivacy.it/regolamentoue/databreach.

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più “copie” dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).
- La risposta fornita all'interessato non deve essere solo “intelligibile”, ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Titolare, responsabile, incaricato del trattamento

Il regolamento

- disciplina la contitolarità del trattamento (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;
- fissa più dettagliatamente (rispetto al Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;
- consente la nomina di sub-responsabili del trattamento da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);
- prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un RPD-DPO (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati recentemente adottate dal Gruppo "Articolo 29", qui disponibili: www.garante-privacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.

Responsabile della protezione dei dati

Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile. Non è un caso, infatti, che fra i compiti del RPD la sorveglianza sull'osservazione del regolamento, informazione e dello svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali).

Decalogo del Garante

- **Cellulari, tablet e smartphone:** il loro utilizzo deve ritenersi consentito **per uso personale e nel rispetto delle persone.**
- Si possono **registrare le lezioni** (spetta agli studi scolastici decidere come regolamentare l'utilizzo di questi strumenti elettronici compresa la possibilità di vietare del tutto l'uso di essi).
- Si possono **consultare** in classe libri elettronici e testi on line.
- **Divieto di diffondere immagini e video sul Web senza il consenso** delle persone eventualmente riprese. (Si ricorda che la diffusione di immagini che ledono la riservatezza e la dignità delle persone può far incorrere in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati).
- **Temi in classe:** l'insegnante può liberamente assegnare gli alunni temi che riguardano il loro mondo personale senza che ciò possa costituire una violazione della privacy. L'insegnante deve però trovare il giusto equilibrio (in caso di lettura dei temi in classe) tra le esigenze dell'insegnamento e il rispetto della privacy quando nei temi vengono trattati argomenti delicati.
- **Gite scolastiche, saggi e recite:** Non c'è violazione della privacy per le riprese fotografiche e per i video fatti dai genitori durante recite, saggi e gite scolastiche, ma queste immagini possono essere usate solo in ambito familiare. Se si intende pubblicarle nel Web, occorre il **consenso delle persone presenti nei video e nelle foto.**
- E' vietato pubblicare nel **sito della scuola** le generalità di chi è in ritardo nel pagamento della retta del servizio mensa.
- È vietato pubblicare i nominativi di chi **usufruisce gratuitamente della mensa.**
- Nel sito della scuola **gli avvisi devono avere carattere generale** giacché ogni altra comunicazione di carattere personale deve essere trasmessa individualmente.
- **Utilizzo di telecamere:** Pur non essendo vietata l'istallazione all'interno degli istituti, la loro presenza deve essere segnalata con cartelli e, in ogni caso, il funzionamento delle telecamere deve avvenire solo negli orari di chiusura. Se poi le telecamere sono collocate all'esterno della scuola è necessario delimitarne l'angolo visuale. In ogni caso le immagini registrate vanno cancellate dopo 24 ore.
- **Iscrizione on-line:** particolare attenzione deve essere prestata inoltre all'eventuale raccolta di dati sensibili. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa, richiede infatti speciali cautele e può essere effettuato solo se i dati sensibili sono indispensabili per l'attività istituzionale svolta
- **Voti ed esami:** gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal Ministero dell'Istruzione dell'Università e della Ricerca. È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali.
- **Attività di ricerca:** se prevedono l'utilizzo di questionari con raccolta di informazioni personali, è necessaria una preventiva informativa ad alunni e genitori sugli scopi della ricerca, le modalità del trattamento e le misure di sicurezza che vengono adottate.