ordine degli architetti
pianificatori, paesaggisti
e conservatori della provincia
di monza e della brianza

fondazione

ordine degli architetti
pianificatori, paesaggisti
e conservatori della provincia
di monza e della brianza

Seminario

PRIVACY E PROFESSIONISTI ALLA LUCE DEL REGOLAMENTO UE 2016/679

Principi e novità del GDPR

Avv. Piero Oggioni

Ordine Architetti PPC Monza
17 maggio 2018

Riferimenti normativi

Art. 8 par. 1 CEDU (Convenzione Europea dei Diritti dell'Uomo)

"Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza"

Art. 16 par. 1 TFUE (Trattato sul Funzionamento dell'Unione Europea)

"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"

Riferimenti normativi

- **Direttiva 95/46/CE** relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

- **Legge 31 dicembre 1996 n. 675** per attuare in Italia la **Direttiva 95/46/CE**

- **Decreto Legislativo 30 giugno 2003 n. 196 (cd. Codice Privacy)**

GDPR

Regolamento UE 2016/679 – cd. GDPR (General Data Protection Regulation)

Abroga la direttiva CE 95/46 ed è direttamente applicabile negli Stati membri UE dal 25.5.2018.

Obiettivi GDPR:

- **Fissare una disciplina comune europea di tutela dei dati direttamente applicabile negli Stati membri**
- **Eliminare asimmetrie delle normative nazionali per favorire la libera circolazione dei dati e lo sviluppo del mercato unico digitale (e rendere competitive le imprese europee)**
- **Creare fiducia nei cittadini**

Per alcuni aspetti occorre un adeguamento della normativa italiana: attualmente siamo in attesa di un decreto legislativo al fine di specificare alcune norme del GDPR ed abrogare le norme del Codice della Privacy.

GDPR

- Il diritto alla protezione dei dati va bilanciato con altri diritti di soggetti pubblici e privati.
- Adempimenti non formali e astratti: vengono descritte le finalità lasciando al titolare del trattamento di perseguire in concreto dette finalità (**Responsabilizzazione**).
- GDPR si applica al solo trattamento di dati delle persone fisiche viventi.
- GDPR non si applica ad attività di pubblica sicurezza e ad attività personali o domestiche (sì però ai fornitori professionali di mezzi per trattare i dati in ambito personale, es. internet provider).
- GDPR si applica a trattamenti automatizzati e a trattamenti manuali di dati personali contenuti in un archivio o destinati a figurarvi.

Soggetti

- **Interessato:** la persona fisica a cui si riferiscono i dati.
- **Titolare del trattamento**: il soggetto che determina le finalità ed il trattamento di dati personali e che deve attuare e dimostrare la conformità del trattamento al GDPR.

- **Responsabile del trattamento**: il soggetto che tratta dati personali per conto del titolare del trattamento (es. gestore del sito, gestore servizi cloud).

  Designato per iscritto dal titolare con atto o contratto contenente la materia disciplinata, la durata del trattamento, la natura e la finalità, il tipo di dati personali, le categorie di interessati, i diritti e gli obblighi del titolare.

  Il responsabile deve garantire la riservatezza e l'adozione di misure di sicurezza dei dati. Collabora con il titolare per il rispetto del GDPR.

Soggetti

- **Autorizzato al trattamento**: il soggetto autorizzato al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (es. dipendente, collaboratore).

  Il titolare deve fornire formazione e istruzioni all'addetto autorizzato.

  Nel Codice della Privacy si parlava di "incaricato".

- **Rappresentante del trattamento**: la persona fisica o giuridica stabilita nell'Unione Europea che rappresenta il titolare o il rappresentante ai fini degli obblighi del GDPR. Viene designato per iscritto dal titolare o responsabile che non è stabilito nell'UE in relazione a trattamenti che riguardano dati personali di interessati che si trovano nell'UE.

Dati

- «**Dato personale**» = qualunque informazione riguardante una persona fisica identificata o identificabile (es. dati anagrafici, codice fiscale, fotografie, targa veicoli, account email).
- «**Dati genetici**» = dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona e che risultano in particolare dall'analisi di un campione biologico.
- «**Dati biometrici**» = dati personali ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca (es. immagine facciale, impronte).
- «**Dati relativi alla salute**» = dati personali attinenti alla salute fisica o mentale di una persona fisica.

Dati

- « **Categorie particolari di dati»** = dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; dati genetici; dati biometrici; dati relativi alla salute; dati relativi alla vita sessuale o all'orientamento sessuale.

  Il Codice della Privacy parlava di dati sensibili.

  Sono dati che rilevano ai fini dell'applicazione di alcune norme del GDPR (es. per nomina DPO, valutazioni di impatto).

Dati

Dati giudiziari = dati personali relativi a condanne penali, reati, misure di sicurezza

- Sono trattati solo sotto il controllo dell'autorità pubblica

Trattamento dati

- «**Trattamento**» = qualunque operazione o insieme di operazioni, compiute con o senza processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Principi

- **Liceità**
- **Correttezza**
- **Trasparenza**
- **Limitazione delle finalità**
- **Minimizzazione dei dati**
- **Esattezza**
- **Limitazione della conservazione**
- **Integrità e riservatezza**

Liceità del trattamento

- **Consenso** = per una o più finalità specifiche (importanza dell'informativa).
- **Contratto** = necessità di stipulare o eseguire un contratto
- **Obbligo legale** (es. adempimenti fiscali o per antiriciclaggio)
- **Salvaguardia interessi vitali** (dell'interessato o di terzi)
- **Compiti di interesse pubblico connesso all'esercizio di pubblici poteri** (rinvio a norme di dettaglio, es. accesso atti, liste elettorali)
- **Legittimo interesse del titolare**, se non prevale su interessi o libertà fondamentali dell'interessato (es. rapporti con clienti/dipendenti, prevenzione frodi).

Trattamento è lecito anche per finalità diverse rispetto alle finalità oggetto di raccolta purchè ci sia il consenso dell'interessato oppure una norma di legge oppure si tratti di finalità compatibile con quella originaria.

Consenso

- Libero, specifico, chiaro, informato.
- Informativa con linguaggio semplice e comprensibile.
- La richiesta di consenso deve essere distinta rispetto ad altre questioni e senza preselezione di caselle.
- Informativa deve chiarire che il consenso può sempre essere revocato.
- Esplicito per le “categorie particolari di dati”.
- Per i minori di 16 anni occorre il consenso dei genitori.

Categorie particolari di dati

Trattamento possibile se:

- Consenso esplicito per finalità specifiche
- Obblighi di diritto di lavoro, sicurezza e protezione sociale
- Interesse vitale dell'interessato o di terzi, quando interessato è incapace di esprimere il consenso
- Da organismi non lucrativi con fini politici, religiosi, filosofici, sindacali se riguarda dati di membri, ex membri, persone con contatti regolari
- Dati resi manifestamente pubblici dall'interessato
- Tutela di diritti in sede giudiziale e stragiudiziale
- Interesse pubblico, proporzionato e con misure appropriate a tutela dell'interessato
- Trattamenti sanitari (medicina preventiva, del lavoro, sanità pubblica)
- Ricerca scientifica, storica e statistica (sempre proporzionato)

Diritti degli interessati

- **Trasparenza** (risposte entro un mese, linguaggio chiaro e semplice)
- **Informativa** (anche con icone)
- **Accesso** (consegna di copia dei dati, consultazione da remoto)
- **Rettifica** (titolare deve comunicare rettifica ai destinatari)
- **Oblio** (deindicizzazione)
- **Limitazione del trattamento**
- **Portabilità dei dati** (solo per trattamenti automatizzati, trasferimento di pacchetto dati ad un altro titolare, es. portabilità numero di telefono)
- **Opposizione al trattamento** (es. per marketing diretto)

In caso di decisione basata su trattamento automatizzato (es. profilazione) = diritto di ottenere intervento umano, di esprimere la propria opinione e di contestare la decisione.

Informativa

Contiene:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) gli eventuali legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;

Informativa

g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

i) qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

l) il diritto di proporre reclamo a un'autorità di controllo;

Informativa

m) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

n) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente .

Privacy by design and by default

- **Privacy by design**

Protezione dei dati sin dalla progettazione del trattamento

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati.

Privacy by design and by default

- **Privacy by default**

Protezione dei dati per impostazione predefinita

Il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità** del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Accountability

- **Responsabilizzazione del titolare**

Al titolare è affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento, nel rispetto del GDPR.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, 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.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure includono l'attuazione di **politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.

Possibilità di aderire a codici di condotta e certificazioni volontarie.

Data Protection Officer (DPO)

- Responsabile della protezione dei dati.

Figura dotata di conoscenza specialistica che assiste il titolare e contribuisce ad integrarne la «responsabilizzazione».

Può essere un dipendente o un soggetto esterno e deve essere indicato nell'informativa e comunicato al Garante.

E' autonomo nell'esecuzione dei compiti e deve avere risorse adeguate.

Non deve essere in conflitto di interessi, cioè non deve rivestire un ruolo decisionale che comporti la definizione delle finalità e modalità del trattamento del titolare.

Data Protection Officer (DPO)

Obbligatorio per:

a) Autorità pubblica;

b) Soggetto privato le cui attività principali consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico** degli interessati **su larga scala**;

c) Soggetto privato le cui attività principali consistono nel trattamento, **su larga scala**, di «categorie particolari di dati personali» o di dati giudiziari.

Data Protection Officer (DPO)

«Larga scala» : si considerano il numero degli interessati, la massa di dati, la tipologia di dati, la durata del trattamento, l'estensione geografica del trattamento.

Es. ospedali, istituti di credito, compagnie assicurative, società di telecomunicazioni, call center.

Per il Garante non dovrebbe essere obbligatorio il DPO per i trattamenti effettuati da liberi professionisti individuali, agenti, imprese familiari.

Data Protection Officer (DPO)

Compiti del DPO:

a) informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR;

b) sorvegliare l'osservanza delle norme relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

d) cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo.

Registri delle attività di trattamento

- Documentazione scritta (anche in formato elettronico) per dimostrare la conformità al GDPR, da mettere a disposizione in casi di controllo.
- Ricognizione dei trattamenti svolti, necessaria per una analisi aggiornata dei rischi e delle conseguenti misure.
- Non obbligatori per organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di «categorie particolari di dati» o di dati giudiziari.

Comunque sempre consigliabili ai fini della cd. Accountability

Registri delle attività di trattamento

Contengono:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Sicurezza dati e valutazione rischi

La valutazione dei rischi è necessaria per realizzare misure adeguate a limitare i rischi di distruzione accidentale o illegale dei dati, perdita, modifica, divulgazione o accesso non autorizzato.

Misure tecniche e organizzative adeguate per garantire un livello di sicurezza soddisfacente, che comprendono se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Valutazione d'impatto sulla protezione dati

- Ulteriore rispetto alla analisi dei rischi che ogni titolare deve effettuare nel progettare e mappare i trattamenti.
- Riguarda i «rischi elevati».

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, **una valutazione dell'impatto** dei trattamenti previsti sulla protezione dei dati personali.

Valutazione d'impatto sulla protezione dati

E' richiesta in particolare in questi casi:

a) una valutazione **sistematica e globale** di aspetti personali relativi a persone fisiche, **basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici** o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, **su larga scala**, di categorie particolari di dati personali o di dati giudiziari;

c) **la sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

E' compito del Garante redigere un elenco delle tipologie di trattamenti soggetti a valutazione di impatto.

Valutazione d'impatto sulla protezione dati

La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Se all'esito della valutazione di impatto emerge che il rischio sulla protezione dati non può essere ragionevolmente attenuato è necessario consultare il Garante prima del trattamento.

Data Breach

In caso di violazione dei dati personali, il titolare del trattamento **notifica la violazione all'autorità di controllo** senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Data Breach

La notifica deve almeno:

a) descrivere **la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati** in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere **le probabili conseguenze** della violazione dei dati personali;

d) descrivere **le misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Data Breach

Quando la violazione dei dati personali è suscettibile di presentare **un rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica senza ingiustificato ritardo, con un linguaggio semplice e chiaro, **la violazione all'interessato**, unitamente al nominativo del DPO, alle probabili conseguenze della violazione dei dati, alle misure adottate per porre rimedio.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento **ha messo in atto le misure tecniche e organizzative adeguate di protezione** e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, **quali la cifratura**;

b) il titolare del trattamento **ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato** per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica.

Responsabilità

- Reclamo al Garante.
- Ricorso innanzi al Giudice.

- Azione di risarcimento danni contro il titolare del trattamento o il responsabile del trattamento.

Un titolare coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il GDPR. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Responsabilità

- Il titolare o il responsabile del trattamento è **esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile**.
- Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato.
- **Rivalsa interna** tra i vari soggetti tenuti al risarcimento, **in proporzione della rispettiva quota** di responsabilità.

Sanzioni

- Sanzioni amministrative pecuniarie:

- Per alcune violazioni fino a 10.000.000 € o, per le imprese, fino al 2% del fatturato mondiale annuo;
- Per altre violazioni fino a 20.000.000 € o, per le imprese, fino al 4% del fatturato mondiale annuo.

Sanzioni inflitte dal Garante in funzione del singolo caso, in modo da essere **effettive, proporzionate e dissuasive**, tenuto conto, tra l'altro, di: natura, gravità e durata della violazione; numero di interessati lesi dal danno e livello del danno da essi subito; carattere doloso o colposo della violazione; misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; grado di responsabilità; eventuali precedenti violazioni pertinenti commesse; grado di cooperazione con l'autorità di controllo al fine di porre rimedio; le categorie di dati personali interessate dalla violazione; l'adesione ai codici di condotta o ai meccanismi di certificazione approvati.

Sanzioni

- Sanzioni penali

Devono essere stabilite dal legislatore nazionale, che deve anche chiarirne l'ambito evitando duplicazioni punitive (amministrative e penali) per i medesimi fatti.

COMUNICAZIONE 24.1.2018 DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO.

« Il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995.

La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento.

Il regolamento produce effetti per la maggior parte degli operatori le cui attività principali consistono nel trattamento dei dati e/o nel trattamento di dati sensibili, nonché per gli operatori che si occupano del monitoraggio regolare e sistematico delle persone fisiche su larga scala ».

GRAZIE PER L'ATTENZIONE