MATERIALE DIDATTICO

PILLOLA 8

COMPITI DEL TITOLARE: PRIVACY BY DESIGN E PRIVACY BY DEFAULT

UNIVERSITÀ TELEMATICA
INTERNAZIONALE UNINETTUNO

in collaborazione con

HUMAN KNOWLEDGE AS OPPORTUNITY

UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO

8 COMPITI DEL TITOLARE: PRIVACY BY DESIGN E PRIVACY BY DEFAULT

in collaborazione con HKAO HUMAN KNOWLEDGE AS OPPORTUNITY

il titolare del trattamento deve attuare misure tecniche e organizzative adeguate

il titolare deve considerare

stato dell'arte in ambito tecnologico

il titolare deve considerare

presumibili costi ed oneri di attuazione

il titolare deve considerare

natura del trattamento

il titolare deve considerare

ambito di applicazione

il titolare deve considerare

contesto e finalità del trattamento

il titolare deve considerare

rischi per diritti e libertà

il titolare deve fare queste valutazioni

al momento della scelta dei mezzi da utilizzare

il titolare deve fare queste valutazioni costantemente nel corso delle attività di trattamento

l'articolo 25 prospetta due metodologie di approccio alla riservatezza dei dati

queste due metodologie di approccio alla privacy possono essere "miscelate" tra loro...

privacy
by design
protezione
dei dati fin
dalla fase di
progettazione

abito sartoriale

privacy
by default
protezione
dei dati per
impostazione
predefinita

abito pret-a-porter

privacy
by design

privacy
software
oriented

privacy by default

condizioni standard idonee

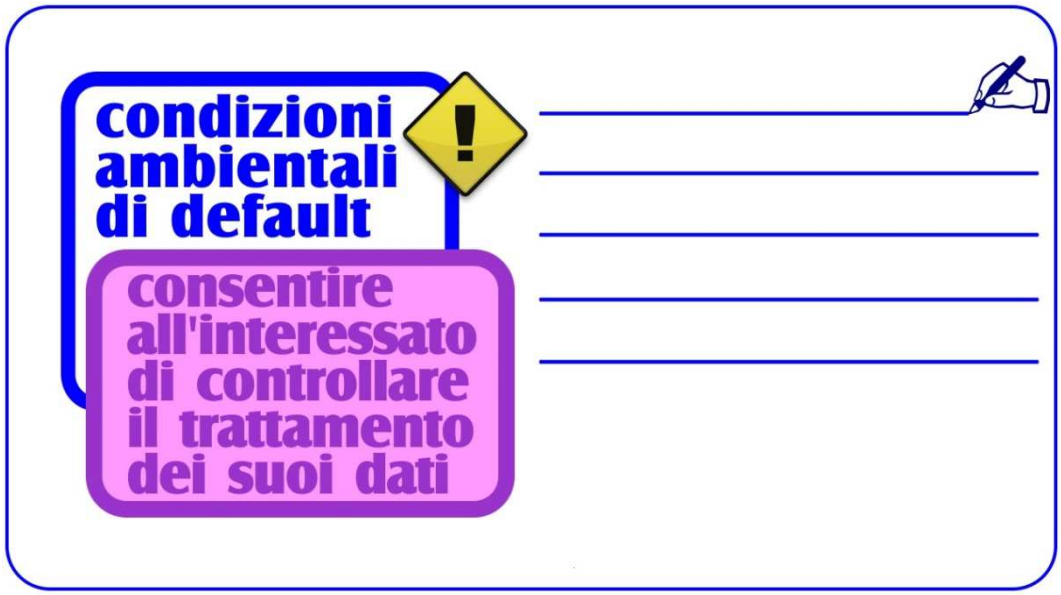
condizioni ambientali di default

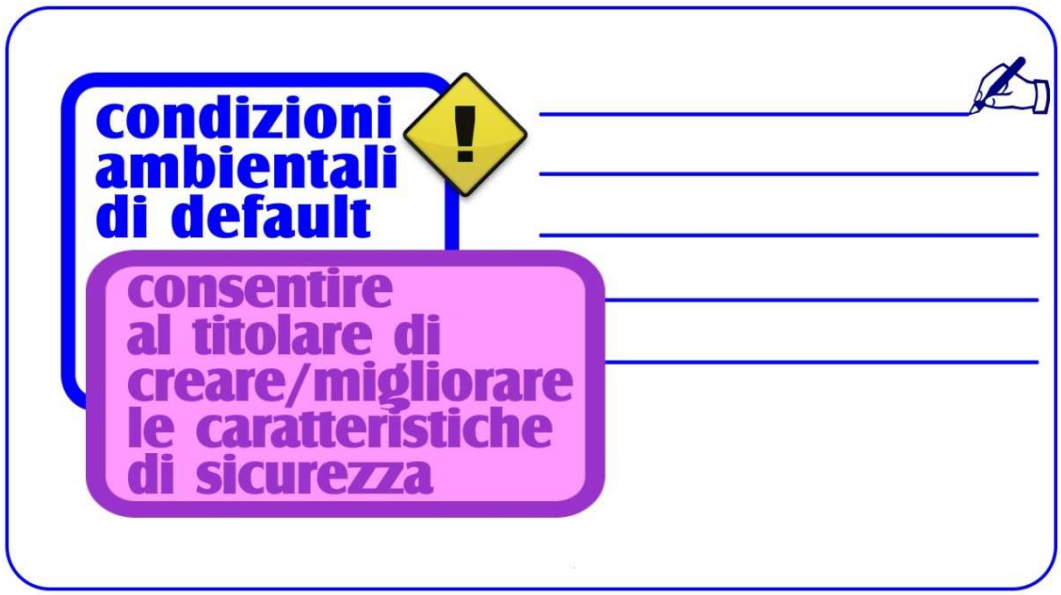
ridurre al minimo il trattamento di dati personali

condizioni ambientali di default

pseudonimizzare i dati personali il prima possibile


condizioni ambientali di default
offrire massima trasparenza per quanto riguarda funzioni/attività del trattamento


condizioni ambientali di default
consentire all'interessato di controllare il trattamento dei suoi dati


condizioni ambientali di default
consentire al titolare di creare/migliorare le caratteristiche di sicurezza

la privacy by default chiama in causa chi produce prodotti, servizi e applicazioni

chi sviluppa soluzioni per il trattamento dei dati dovrebbe considerare la privacy già in fase di...

sviluppo

chi sviluppa soluzioni per il trattamento dei dati dovrebbe considerare la privacy già in fase di...

progettazione

chi sviluppa soluzioni per il trattamento dei dati dovrebbe considerare la privacy già in fase di...

selezione/uso di applicazioni

i principi della privacy by design e by default dovrebbero essere valutati nell'aggiudicare appalti pubblici

la c.d. "privacy by default" è applicabile esclusivamente per trattare i dati personali indispensabili per ogni specifica finalità

tale obbligo vale in ragione di

quantità di dati raccolti

tale obbligo vale in ragione di

portata del trattamento

tale obbligo vale in ragione di

periodo di conservazione

tale obbligo vale in ragione di

accessibilità

i dati personali non devono essere accessibili a un numero indefinito di soggetti...

...senza che vi sia l'intervento materiale di un operatore incaricato del trattamento


un meccanismo
di certificazione
può essere
utilizzato
per dimostrare
la conformità
a legge della
privacy by default
e by design
APPROVED

REGOLAMENTO (UE) 2016/679
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

(Testo rilevante ai fini del SEE)

Articolo 25
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
(riferimento ai "considerando" C75-78)

1. 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 presente regolamento e tutelare i diritti degli interessati.
2. 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.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

estratto dei “considerando” richiamati a margine delle norme

in riferimento all’articolo 25 del Regolamento 679/2016

(75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d’identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l’esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l’analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

(76) La probabilità e la gravità del rischio per i diritti e le libertà dell’interessato dovrebbero essere determinate con riguardo alla natura, all’ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

(77) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l’individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l’individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio.

(78) La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l’adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l’altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all’interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell’arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell’ambito degli appalti pubblici.