General Data Protection Regulation

Zan ! Zan !

Michele Finelli
m@biodec.com
BioDec

Ovvero

REGOLAMENTI

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)

Indice

Che cos'è in poche parole

- Una legge.
- Più precisamente **un regolamento europeo**, il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.
- È entrato ufficialmente in vigore il 24 maggio 2016.
- Diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

In *in testo slanted* quanto preso dal sito del Garante.

Che cos'è in poche parole

- Una legge.
- Più precisamente **un regolamento europeo**, il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.
- È entrato ufficialmente in vigore il 24 maggio 2016.
- Diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

In *in testo slanted* quanto preso dal sito del Garante.

Che cos'è in poche parole

- Una legge.
- Più precisamente **un regolamento europeo**, il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.
- È entrato ufficialmente in vigore il 24 maggio 2016.
- Diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

In *in testo slanted* quanto preso dal sito del Garante.

Che cos'è in poche parole

- Una legge.
- Più precisamente **un regolamento europeo**, il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.
- È entrato ufficialmente in vigore il 24 maggio 2016.
- Diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

In *in testo slanted* quanto preso dal sito del Garante.

Che cos'è in poche parole

- Una legge.
- Più precisamente **un regolamento europeo**, il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.
- È entrato ufficialmente in vigore il 24 maggio 2016.
- Diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

In *in testo slanted* quanto preso dal sito del Garante.

Che cos'è in poche parole

- Una legge.
- Più precisamente **un regolamento europeo**, il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.
- È entrato ufficialmente in vigore il 24 maggio 2016.
- Diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

In *in testo slanted* quanto preso dal sito del Garante.

Cosa comporta per il cittadino

1. *Il regolamento introduce regole più chiare in materia di informativa e consenso,*
2. *definisce i limiti al trattamento automatizzato dei dati personali,*
3. *pone le basi per l'esercizio di nuovi diritti,*
4. *stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach).*

Cosa comporta per il cittadino

1. *Il regolamento introduce regole più chiare in materia di informativa e consenso,*
2. *definisce i limiti al trattamento automatizzato dei dati personali,*
3. *pone le basi per l'esercizio di nuovi diritti,*
4. *stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach).*

Cosa comporta per il cittadino

1. *Il regolamento introduce regole più chiare in materia di informativa e consenso,*
2. *definisce i limiti al trattamento automatizzato dei dati personali,*
3. *pone le basi per l'esercizio di nuovi diritti,*
4. *stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach).*

Cosa comporta per il cittadino

1. *Il regolamento introduce regole più chiare in materia di informativa e consenso,*
2. *definisce i limiti al trattamento automatizzato dei dati personali,*
3. *pone le basi per l'esercizio di nuovi diritti,*
4. *stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach).*

Cosa comporta per il cittadino

1. *Il regolamento introduce regole più chiare in materia di informativa e consenso,*
2. *definisce i limiti al trattamento automatizzato dei dati personali,*
3. *pone le basi per l'esercizio di nuovi diritti,*
4. *stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach).*

Gestione dei consensi

- *Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).*
- *Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.*
- *Il consenso potrà essere revocato in ogni momento.*

Gestione dei consensi

- *Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).*
- *Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.*
- *Il consenso potrà essere revocato in ogni momento.*

Gestione dei consensi

- *Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).*
- *Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.*
- *Il consenso potrà essere revocato in ogni momento.*

Gestione dei consensi

- *Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).*
- *Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.*
- *Il consenso potrà essere revocato in ogni momento.*

Cosa comporta per chi tratta dati personali

In ordine sparso:

- Nuove figure (il *Data Protection Officer*).
- Obbligo di comunicare i casi di violazione dei dati personali (data breach).
- Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste delle sanzioni molto elevate — ad esempio fino a 20.000.000€ o il 4% del fatturato mondiale totale annuo.

Cosa comporta per chi tratta dati personali

In ordine sparso:

- Nuove figure (il *Data Protection Officer*).
- Obbligo di comunicare i casi di violazione dei dati personali (data breach).
- Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste delle sanzioni molto elevate — ad esempio fino a 20.000.000€ o il 4% del fatturato mondiale totale annuo.

Cosa comporta per chi tratta dati personali

In ordine sparso:

- Nuove figure (il *Data Protection Officer*).
- Obbligo di comunicare i casi di violazione dei dati personali (data breach).
- Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste delle sanzioni molto elevate — ad esempio fino a 20.000.000€ o il 4% del fatturato mondiale totale annuo.

Cosa comporta per chi tratta dati personali

In ordine sparso:

- Nuove figure (il *Data Protection Officer*).
- Obbligo di comunicare i casi di violazione dei dati personali (data breach).
- Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste delle sanzioni molto elevate — ad esempio fino a 20.000.000€ o il 4% del fatturato mondiale totale annuo.

Altri diritti (e doveri)

- Articolo 7 “(. . .) L’interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.” e poi gli articoli 15 e 16.
- Articolo 17 “Diritto all’oblio”.
- Articolo 25. “(. . .) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (. . .) volte ad attuare in modo efficace i principi di protezione dei dati (. . .)”

Altri diritti (e doveri)

- Articolo 7 “(. . .) L’interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.” e poi gli articoli 15 e 16.
- Articolo 17 “Diritto all’oblio”.
- Articolo 25. “(. . .) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (. . .) volte ad attuare in modo efficace i principi di protezione dei dati (. . .)”

Altri diritti (e doveri)

- Articolo 7 “(. . .) L’interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.” e poi gli articoli 15 e 16.
- Articolo 17 “Diritto all’oblio”.
- Articolo 25. “(. . .) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (. . .) volte ad attuare in modo efficace i principi di protezione dei dati (. . .)”

Altri diritti (e doveri)

- Articolo 7 “(. . .) L’interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.” e poi gli articoli 15 e 16.
- Articolo 17 “Diritto all’oblio”.
- Articolo 25. “(. . .) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (. . .) volte ad attuare in modo efficace i principi di protezione dei dati (. . .)”

Altri diritti (e doveri)

- Articolo 30. “Registri delle attività di trattamento”
- Articoli 33 e 34 riguardo la notifica e la comunicazione di una violazione.
- Sezione 3 “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva”

Altri diritti (e doveri)

- Articolo 30. “Registri delle attività di trattamento”
- Articoli 33 e 34 riguardo la notifica e la comunicazione di una violazione.
- Sezione 3 “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva”

Altri diritti (e doveri)

- Articolo 30. “Registri delle attività di trattamento”
- Articoli 33 e 34 riguardo la notifica e la comunicazione di una violazione.
- Sezione 3 “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva”

Altri diritti (e doveri)

- Articolo 30. “Registri delle attività di trattamento”
- Articoli 33 e 34 riguardo la notifica e la comunicazione di una violazione.
- Sezione 3 “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva”

Indice

Cosa c'entra il *software libero*

Apparentemente nulla. Ma non fermiamoci alle apparenze.

Cosa c’entra il *software libero*

Apparentemente nulla. Ma non fermiamoci alle apparenze.

Privacy by design

- *Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.*
- *Il principio-chiave è privacy by design, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problemi.*

Privacy by design

- *Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.*
- *Il principio-chiave è privacy by design, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problemi.*

Privacy by design

- *Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.*
- *Il principio-chiave è privacy by design, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problemi.*

Codici di condotta e certificazioni

L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

Approccio metodologico $\Longrightarrow$ implicazioni pratiche

- Uno dei concetti spesso ribaditi, sotto diverse forme, è quello della necessità di un approccio metodologico, ovvero di un **processo di gestione dei dati personali**.
- Inoltre: si enfatizza che le misure devono essere **adeguate** — non, come in altri casi "minime". Cioè, in qualche modo si vuole rimarcare che si chiede che le cose **funzionino**.
- Non solo, se il processo **è certificato** si ha la possibilità di non dovere ottemperare a certi obblighi.

Approccio metodologico $\Longrightarrow$ implicazioni pratiche

- Uno dei concetti spesso ribaditi, sotto diverse forme, è quello della necessità di un approccio metodologico, ovvero di un **processo di gestione dei dati personali**.
- Inoltre: si enfatizza che le misure devono essere **adeguate** — non, come in altri casi "minime". Cioè, in qualche modo si vuole rimarcare che si chiede che le cose **funzionino**.
- Non solo, se il processo **è certificato** si ha la possibilità di non dovere ottemperare a certi obblighi.

Approccio metodologico $\Longrightarrow$ implicazioni pratiche

- Uno dei concetti spesso ribaditi, sotto diverse forme, è quello della necessità di un approccio metodologico, ovvero di un **processo di gestione dei dati personali**.
- Inoltre: si enfatizza che le misure devono essere **adeguate** — non, come in altri casi "minime". Cioè, in qualche modo si vuole rimarcare che si chiede che le cose **funzionino**.
- Non solo, se il processo **è certificato** si ha la possibilità di non dovere ottemperare a certi obblighi.

Approccio metodologico $\Longrightarrow$ implicazioni pratiche

- Uno dei concetti spesso ribaditi, sotto diverse forme, è quello della necessità di un approccio metodologico, ovvero di un **processo di gestione dei dati personali**.
- Inoltre: si enfatizza che le misure devono essere **adeguate** — non, come in altri casi “minime”. Cioè, in qualche modo si vuole rimarcare che si chiede che le cose **funzionino**.
- Non solo, se il processo **è certificato** si ha la possibilità di non dovere ottemperare a certi obblighi.

Il vantaggio del software libero e dei formati aperti

- In alcuni casi il basarsi su standard aperti è ormai una prassi non più discutibile: chi userebbe un algoritmo di cifratura proprietario ?
- Se si vuole dimostrare[1] la correttezza di un certo sistema informatico, poterci guardare dentro sembrerebbe “una misura minima”.
- Se i dati devono essere “portabili” (Articolo 20), è difficile immaginare come questi possano essere gestiti tramite dei formati chiusi.

[1] Per valori ampi di “dimostrare”.

Il vantaggio del software libero e dei formati aperti

- In alcuni casi il basarsi su standard aperti è ormai una prassi non più discutibile: chi userebbe un algoritmo di cifratura proprietario ?
- Se si vuole dimostrare[1] la correttezza di un certo sistema informatico, poterci guardare dentro sembrerebbe “una misura minima”.
- Se i dati devono essere “portabili” (Articolo 20), è difficile immaginare come questi possano essere gestiti tramite dei formati chiusi.

[1] Per valori ampi di “dimostrare”.

Il vantaggio del software libero e dei formati aperti

- In alcuni casi il basarsi su standard aperti è ormai una prassi non più discutibile: chi userebbe un algoritmo di cifratura proprietario ?
- Se si vuole dimostrare[1] la correttezza di un certo sistema informatico, poterci guardare dentro sembrerebbe “una misura minima”.
- Se i dati devono essere “portabili” (Articolo 20), è difficile immaginare come questi possano essere gestiti tramite dei formati chiusi.

[1] Per valori ampi di “dimostrare”.

Il vantaggio del software libero e dei formati aperti

- In alcuni casi il basarsi su standard aperti è ormai una prassi non più discutibile: chi userebbe un algoritmo di cifratura proprietario ?
- Se si vuole dimostrare[1] la correttezza di un certo sistema informatico, poterci guardare dentro sembrerebbe “una misura minima”.
- Se i dati devono essere “portabili” (Articolo 20), è difficile immaginare come questi possano essere gestiti tramite dei formati chiusi.

[1] Per valori ampi di “dimostrare”.

Thanks

Piccola pubblicità progresso:

- 25 novembre 2017 - No Slides Conf, a Bologna.
- http://www.noslidesconf.net