CONFERIMENTO DELL'INCARICO PER L'ATTUAZIONE DEL REGOLAMENTO U.E n. 679/2016 SULLA PROTEZIONE DEI DATI PERSONALI
ED
INDIVIDUAZIONE RESPONSABILE PROTEZIONE DATI (RPD)

Disciplinare tecnico

A. Indicazioni generali

Il Regolamento Generale sulla Protezione dei dati personali (Regolamento UE 679/2016 detto anche "RGPD") è un atto con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all'interno che all'esterno dei confini dell'Unione europea.
Il testo, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Le disposizioni contenute nel nuovo Regolamento europeo per la protezione dei dati personali impongono di assicurare, entro il 25 maggio 2018, l'applicazione tassativa della normativa europea sul trattamento dei dati, la cui responsabilità ultima cade sul titolare del trattamento, figura che nella FBRB è ricoperta dalla Presidente.

L'adozione delle disposizioni contenute nel Regolamento europeo inciderà notevolmente sull'organizzazione interna e richiederà la ricognizione, la valutazione e l'eventuale adeguamento delle misure di sicurezza normative, organizzative e tecnologiche.
Il modello immaginato dal legislatore Europeo passa attraverso le seguenti fasi:

- un'analisi del contesto, con la mappatura dei processi soggetti a rischio, e rilevazione dei livelli di sicurezza oggi esistenti, sia dal punto di vista informatico sia dal punto di vista analogico;
- la definizione e pianificazione delle misure necessarie al raggiungimento di un adeguato livello di sicurezza, conforme agli standards previsti;
- l'implementazione di un sistema di "autocontrollo", che preveda il continuo monitoraggio, l'aggiornamento e l'implementazione delle misure di sicurezza, e la documentazione di tutta l'attività che viene svolta a tali fini;
- la formazione periodica degli operatori dei diversi settori interessati, al fine di accrescere la consapevolezza dei rischi ed aumentare la capacità di prevenzione.
- l'individuazione e nomina del RPD (Responsabile Protezione Dati)

L'attività da svolgere presuppone quindi l'incrocio di competenze informatiche e giuridiche:

- comprovate competenze giuridiche, con particolare riguardo al diritto amministrativo e alle norme sulla tutela dei dati personali; le competenze sono documentabili dal possesso della laurea in materie giuridiche e/o dall'esperienza lavorativa maturata presso enti privati e/o enti locali o altre pubbliche amministrazioni, in qualità di dipendenti, consulenti o collaboratori.
- comprovate competenze informatiche, con particolare riguardo alla gestione di sistemi informativi complessi, afferenti al trattamento di dati personali; le competenze sono documentabili dal possesso di titolo di studio adeguato e/o dall'esperienza

lavorativa maturata presso aziende private, enti locali o altre pubbliche amministrazioni, in qualità di dipendenti, consulenti o collaboratori nel settore informatico.

B. Organizzazione amministrativa

La struttura della FBRB è così articolata:

- ✓ Presidente
- ✓ Consiglio di Amministrazione
- ✓ Direzione Amministrativa
- ✓ Revisore Contabile
- ✓ Comitato Scientifico e di Coordinamento

C. Ubicazione fisica degli uffici e servizi

Gli uffici della FBRB, ad oggi, sono dislocati:

- n. 1 presso il Palazzo della Giunta della Regione Basilicata;
- n. 1 presso l'Ospedale Madonna delle Grazie di Matera.

D. Trattamenti di dati

Il trattamento viene effettuato per lo più con modalità informatizzate preceduto dal consenso degli interessati.

E. Organizzazione informatica

Il sistema informatico consta di n. 2 computer.

F. Oggetto dell'incarico

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal citato Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del citato regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento 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;
- fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del citato Regolamento ;
- cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del citato Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
- Mappatura processi e trattamenti;
- Individuazione aree di rischio;
- Supporto alla predisposizione delle misure di miglioramento dei processi;
- Gestione del registro/i dei trattamenti;
- Gestione registro violazioni di sicurezza e relativa modulistica;

- Elaborazione modulistica per incarichi e schemi negoziali (ad uso : interessati; delegati; RDP; responsabili del trattamento etc.);
- Definizione indirizzi formativi per il personale interessato;
- proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni.
- Attività collaterali alle precedenti.

G. Contenuti e tempistica

1. Nomina del RDP

La nomina del RDP avrà decorrenza dalla data di conferimento dell'incarico (25/05/2018) e durata biennale.

Compiti del Responsabile della Protezione dei Dati

L'istituzione della nuova figura del *Responsabile della protezione dei dati* (in seguito indicato con "RPD") è la principale novità normativa del Regolamento europeo che mira la potenziamento del controllo dell'efficacia e della sicurezza dei sistemi di protezione dei dati personali.

Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:

a. Informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. Ai fini del presente compito il RPD deve indicare al Titolari i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b. Sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare del trattamento;
c. Sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
d. fornire parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA), fornire gli opportuni suggerimenti per lo svolgimento delle attività nel modo più sicuro e meno impattante, sorvegliarne lo svolgimento;
e. cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità;
f. provvedere alla tenuta dei registri dei trattamenti dati personali.
g. supportare il Titolare e i Responsabili del trattamento nell'individuare processi organizzativi idonei a contemperare le esigenze della gestione delle attività di competenza e le esigenze di tutela dei dati;

Mappatura dei processi, individuazione dei rischi e mappatura degli incarichi

L'attività di mappatura dei processi, degli incaricati e l'individuazione del livello di protezione o di rischio sono il punto di partenza per definire la situazione di partenza e la strada da percorrere per raggiungere gli obiettivi previsti dal legislatore europeo.

Le attività previste dai punti precedenti devono concludersi entro 30 giorni naturali e consecutivi dal conferimento dell'incarico.

Elaborazione del piano di adeguamento

Il piano di adeguamento contiene le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi (se necessario) e dei tempi previsti, nonché delle attività di monitoraggio e le tempistiche.
Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono, a titolo esemplificativo: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Costituiscono altresì misure tecniche ed organizzative i sistemi di autenticazione; i sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro); le misure antincendio; i sistemi di rilevazione di intrusione; i sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

Interventi formativi del personale

Gli interventi formativi del personale devono prevedere una formazione di base, da impartire a tutti i dipendenti, e di una formazione specialistica per i dipendenti che svolgono attività classificate a rischio più elevato. Il piano di formazione dovrà essere presentato in contemporanea al piano di adeguamento, e dovrà essere programmato in modo da fare fronte alle carenze riscontrate nell'ambito della mappatura. Il calendario e le modalità di articolazione della formazione saranno concordati con il Titolare del trattamento o suo delegato, e/o, in caso di formazione riguardante specifici settori, con il dirigente competente.

Predisposizione e tenuta del registro dei trattamenti di dati personali e del registro delle categorie di attività

Il Registro delle attività di trattamento dovrà prevedere almeno le seguenti informazioni:

a. il nome ed i dati di contatto della FBRB, eventualmente del Contitolare del trattamento, del RPD;
b. le finalità del trattamento;
c. la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute);

d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario;
e. l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;
f. ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate;

h. Registro delle categorie di attività
    a. Il Registro delle categorie di attività, trattate da ciascun Responsabile del trattamento dovrà prevedere le seguenti informazioni:
        i. il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
        ii. le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione;
        iii. l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione
        iv. internazionale;
        v. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate

La predisposizione dei registri sarà a cura del RDP, non appena conclusa la fase di mappatura prevista.
La tenuta e l'aggiornamento dei registri sarà a cura del RDP che dovrà provvedervi tempestivamente; con cadenza semestrale i registri dovranno essere sottoposti al controllo ed alla vidimazione, rispettivamente:

- ✓ per quanto riguarda il registro dei trattamenti, al titolare del trattamento o suo delegato
- ✓ per quanto riguarda il registro delle categorie di attività trattate, ai dirigenti dei servizi competenti

<u>Proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni</u>
La proposta di adeguamento della modulistica in uso agli uffici, se non conforme alle nuove disposizioni, dovrà essere completata entro due mesi dalla data di scadenza dei termini per la mappatura.

<u>Valutazione di impatto sulla protezione dei dati</u>
Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, su segnalazione del Responsabile del trattamento, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
Il Titolare si avvale della consulenza tecnica del RDP, il quale dovrà fornire i seguenti elementi, entro 15 giorni dalla richiesta: descrivere il trattamento, valutarne necessità e

proporzionalità, individuare le migliori modalità di gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali e permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

H. Inadempimento e ritardo – penalità

Il ritardo nell'esecuzione delle prestazioni indicate al punto precedente e nella predisposizione dei registri previsti comporterà l'applicazione di una penale giornaliera di € 100,00 per ogni giorno lavorativo di ritardo.

Il ritardo nell'esecuzione delle altre prestazioni previste dal capitolato comporterà l'applicazione di una penale giornaliera di € 50,00 per ogni giorno lavorativo di ritardo.

In ogni caso, qualora il ritardo superi i 15 giorni, si farà luogo alla risoluzione del contratto, ai sensi degli articoli 1453 e 1454 del codice civile, con richiesta di risarcimento dei danni.

L'applicazione della penale sarà preceduta da formale contestazione scritta; l'aggiudicatario avrà la facoltà di presentare le proprie contro-deduzioni nel termine indicato nella contestazione, non inferiore a 10 giorni dalla data del ricevimento della contestazione stessa.

Qualora entro il termine stabilito l'aggiudicatario non fornisca alcuna motivata giustificazione scritta, ovvero qualora le stesse non fossero ritenute accoglibili, la FBRB applicherà le penali previste, motivando adeguatamente in ordine al mancato accoglimento delle giustificazioni.

Non è comunque precluso alla FBRB il diritto di sanzionare eventuali casi non espressamente contemplati, ma comunque rilevanti rispetto alla corretta erogazione del servizio.

L'importo complessivo delle penali irrogate ai sensi dei commi precedenti non può superare il 10 % dell'importo contrattuale aggiudicato. Qualora le inadempienze siano tali da comportare il superamento di tale importo trova applicazione quanto previsto in materia di risoluzione del contratto.

Il provvedimento applicativo della penale sarà assunto dalla FBRB e comunicato all'Aggiudicatario. L'importo relativo all'applicazione della penale, esattamente quantificato nel provvedimento applicativo della stessa penalità, verrà detratto dal pagamento della fattura emessa.

I. Risoluzione per grave inadempienza – clausola risolutiva espressa

Nel caso di inadempienze gravi e/o ripetute agli obblighi previsti dal presente capitolato, diversi da quelli già previsti dall'articolo precedente, la FBRB ha la facoltà, previa contestazione scritta, di risolvere il contratto, ai sensi degli articoli 1453 e 1454 del codice civile, con tutte le conseguenze di legge che la risoluzione comporta. Ai fini del presente comma, si intendono inadempienze gravi:

- ✓ l'inosservanza degli obblighi derivanti dalla qualifica di RDP
- ✓ il mancato e reiterato aggiornamento tempestivo dei registri di cui al punto "G";
- ✓ lo svolgimento dei doveri derivanti dal presente incarico senza la necessaria diligenza e perizia tecnica e giuridica, richiesta dalla peculiarità del servizio, che abbia comportato rilievi o sanzioni ad opera delle Autorità competenti al controllo;
- ✓ la cessazione o la sostituzione del RDP

Si applicano alla risoluzione del contratto i principi del giusti procedimenti già previsti nell'articolo precedente in materia di irrogazione delle penali.

J. Obbligo di tracciabilità dei flussi finanziari

L'aggiudicatario assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136 e successive modifiche.

Potenza, 11/05/2018