



REGIONE SICILIANA

GIUNTA REGIONALE

Deliberazione n. 483 del 29 novembre 2018.

“Regolamento UE 2016/679 – Adozione delle prime istruzioni organizzative e tecniche per il trattamento dei dati personali, di una procedura di risposta ad una violazione dei dati personali e di un questionario di autovalutazione”.

La Giunta Regionale

VISTO lo Statuto della Regione;

VISTE le leggi regionali 29 dicembre 1962, n.28 e 10 aprile 1978, n.2;

VISTA la legge regionale 16 dicembre 2008, n.19 e successive modifiche e integrazioni;

VISTO il D.P.Reg. 18 gennaio 2013, n. 6;

VISTO il D.P.Reg. 14 giugno 2016, n. 12 concernente: “Regolamento di attuazione del Titolo II della legge regionale 16 dicembre 2008, n. 19. Rimodulazione degli assetti organizzativi dei Dipartimenti regionali di cui all'articolo 49, comma 1, della legge regionale 7 maggio 2015, n.9. Modifica del decreto del Presidente della Regione 18 gennaio 2013, n. 6, e successive modifiche e integrazioni”, come modificato dal D.P.Reg. 3 agosto 2017, n.18;

VISTO il proprio Regolamento interno;

VISTO il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

VISTO il 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);





REGIONE SICILIANA

GIUNTA REGIONALE

VISTO il decreto legislativo 10 agosto 2018, n. 101 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del citato Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

VISTA la deliberazione della Giunta regionale n. 203 del 28 maggio 2018 e relativo D.P.Reg. di attuazione n. 569 del 12 giugno 2018, con cui l'Ing. Sebastiano Lio, Dirigente dell'Amministrazione regionale, in servizio presso l'Ufficio per l'attività di coordinamento dei sistemi informativi e l'attività informatica della Regione e delle Pubbliche Amministrazioni regionali, è stato nominato quale "Responsabile della protezione dei dati", ai sensi dell'art. 37 del predetto Regolamento UE 2016/679, con i compiti previsti dal successivo art. 39, tra i quali, informare e fornire consulenza ai titolari e ai responsabili del trattamento dei dati personali e sorvegliare l'osservanza del Regolamento medesimo;

CONSIDERATO che il richiamato D.P.Reg. n. 569/2018 prevede, altresì, che il Responsabile della protezione dei dati, nelle more dell'istituzione di una adeguata struttura organizzativa dedicata alla specifica funzione, potrà avvalersi del succitato Ufficio per l'attività di coordinamento dei sistemi informativi e l'attività informatica della Regione e delle Pubbliche Amministrazioni regionali, e del supporto della Segreteria generale della Presidenza della Regione, dell'Ufficio legislativo e legale della Presidenza della Regione e del Dipartimento regionale della funzione pubblica e del personale;

VISTA la nota prot. n. 15003 del 5 novembre 2018 con la quale il Presidente della Regione trasmette, per l'apprezzamento della Giunta regionale, la





REGIONE SICILIANA

GIUNTA REGIONALE

relazione del Responsabile della protezione dei dati della Regione Siciliana, prot. n. 51 del 28 settembre 2018, concernente le prime misure attuative del citato Regolamento UE 2016/679, unitamente ai seguenti documenti: “Prime istruzioni organizzative e tecniche per il trattamento dei dati personali”, “Procedura di risposta ad una violazione dei dati personali” e “Questionario di autovalutazione sulla conformità al Regolamento UE 679/2016 sulla protezione dei dati personali” (Allegato “A”);

CONSIDERATO che, nella predetta relazione prot. n. 51/2018, il Responsabile della protezione dei dati, nel premettere che i documenti sopra richiamati consentono di rendere più efficace l'attività di trattamento dei dati personali svolta negli Uffici e rivelano l'impegno profuso dalla Regione Siciliana per garantire il rispetto delle norme o degli standard in materia di protezione dei dati, mediante l'utilizzo di procedure uniformi per tutta l'Amministrazione regionale, descrive il contenuto degli stessi rappresentando, in particolare, che il primo documento “Prime istruzioni organizzative e tecniche per il trattamento dei dati personali” definisce le politiche interne, uniformi per tutta l'Amministrazione e coerenti con l'attuale quadro legislativo, con riferimento al mutato assetto operativo dell'Amministrazione regionale in tema di protezione dei dati personali, e che nel documento medesimo sono riportate le principali figure coinvolte nella gestione dei dati personali ed i compiti ad esse attribuiti; che il secondo documento “Procedura di risposta ad una violazione dei dati personali” definisce le fasi del processo operativo, uniforme per tutta l'Amministrazione, da seguire nel caso in cui si manifesti una violazione di dati personali, descrivendo gli adempimenti a cui sono tenuti i soggetti





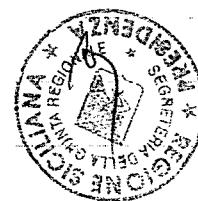
REGIONE SICILIANA

GIUNTA REGIONALE

coinvolti e la sequenza operativa; che, infine, il terzo documento “Questionario di autovalutazione sulla conformità al Regolamento UE 679/2016 sulla protezione dei dati personali” risponde all'esigenza di monitorare dall'interno dell'Amministrazione il rispetto delle politiche in materia di protezione dei dati personali; che detto questionario deve essere compilato semestralmente a cura di ciascun Dipartimento o Ufficio equiparato e consente di monitorare il grado di aderenza dell'attività amministrativa alla norma comunitaria, misurando periodicamente gli sviluppi e rilevando le criticità, al fine di porre in essere gli interventi correttivi;

CONSIDERATO che il Responsabile della protezione dei dati rappresenta, altresì, che gli adempimenti attuativi previsti nei documenti sopra descritti, ed, in particolare, il coordinamento e il monitoraggio della fase attuativa riferita all'uniforme applicazione delle istruzioni organizzative e della procedura, nonché la predisposizione di apposita direttiva contenente indicazioni operative sulla compilazione e la raccolta dei questionari semestrali di autovalutazione dovranno essere curati, per competenza, dal Dipartimento regionale della funzione pubblica e del personale, ed, inoltre, che i documenti in parola sono stati esaminati ed apprezzati positivamente nella riunione del 27 settembre 2018 alla quale hanno partecipato, oltre al Responsabile della protezione dei dati, i rappresentanti della Segreteria generale, del Dipartimento regionale della funzione pubblica e del personale, dell'Ufficio legislativo e legale e dell'Autorità per l'innovazione tecnologica;

RITENUTO di apprezzare i documenti “Prime istruzioni organizzative e tecniche per il trattamento dei dati personali”, “Procedura di risposta ad una





REGIONE SICILIANA

GIUNTA REGIONALE

violazione dei dati personali” e “Questionario di autovalutazione sulla conformità al Regolamento UE 679/2016 sulla protezione dei dati personali”, proposti dal Responsabile della protezione dei dati e concernenti misure attuative del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

SU proposta del Presidente della Regione,

DELIBERA

per quanto esposto in preambolo, di apprezzare i documenti “Prime istruzioni organizzative e tecniche per il trattamento dei dati personali”, “Procedura di risposta ad una violazione dei dati personali” e “Questionario di autovalutazione sulla conformità al Regolamento UE 679/2016 sulla protezione dei dati personali”, concernenti misure attuative del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016. proposti dal Responsabile della protezione dei dati e trasmessi dal Presidente della Regione con nota prot. n. 15003 del 5 novembre 2018, costituenti allegato “A” alla presente deliberazione.

Il Segretario

BUONISI



Il Presidente

MUSUMECI

MTC

ATTI DELLA GIUNTA REGIONALE

Repubblica Italiana



Regione Siciliana

PRESIDENZA
UFFICIO DI GABINETTO

DELIBERAZIONE N. h83 DEL 29.11.18 ALLEGATO A PAQ 101-22

Prot. n° 15003

Palermo, 05.11.2018

OGGETTO: Regolamento UE 2016/679 - Proposta per l'adozione delle prime istruzioni organizzative e tecniche per il trattamento dei dati personali, di una procedura di risposta ad una violazione dei dati personali e di un questionario di autovalutazione.-

Alla Segreteria di Giunta

e, p.c.

All'Assessore regionale
delle Autonomie locali
e della Funzione pubblica

Al Dipartimento regionale
della Funzione pubblica e del Personale

Al Responsabile regionale
per la protezione dei dati
ex Regolamento UE 2016/679

PRESIDENZA REGIONE SICILIANA Segreteria della Giunta Regionale
05 NOV. 2018
PROT. N. <u>3826</u>

Affinchè sia sottoposta all'apprezzamento della Giunta regionale nella prossima seduta utile, si trasmette, unitamente ai relativi allegati, copia della nota del Responsabile della protezione dati della Regione Siciliana prot. n. 51 del 28 settembre 2018, di pari oggetto, al cui contenuto si rinvia, inerente le prime misure attuative del Regolamento UE 2016/679, unitamente ai documenti allegati riguardanti:

- Prime istruzioni organizzative e tecniche per il trattamento dei dati personali;
- Procedura di risposta ad una violazione dei dati personali;
- Questionario di autovalutazione sulla conformità al Regolamento UE 679/2016 sulla protezione dei dati personali.

Tale proposta costituisce un indispensabile adempimento operativo per l'applicazione di misure attuative del Regolamento UE 2016/679 nella Regione Siciliana.



IL SEGRETARIO

5/11/2018

St. 3

Am

DELIBERAZIONE N. h.83 DEL 29.11.18 ALLEGATO A PAQ 2

Repubblica Italiana



Regione Siciliana

PRESIDENZA
UFFICIO DI GABINETTO

Gli adempimenti attuativi previsti negli allegati documenti è, in particolare, il coordinamento e il monitoraggio della fase attuativa riferita all'uniforme applicazione delle istruzioni organizzative e della procedura, nonché la predisposizione di apposita direttiva contenente indicazioni operative sulla compilazione e la raccolta dei questionari semestrali di autovalutazione dovranno essere curati, per competenza, dal Dipartimento regionale della Funzione Pubblica e del Personale.

Il Presidente
MUSUMECI



IL SEGRETARIO

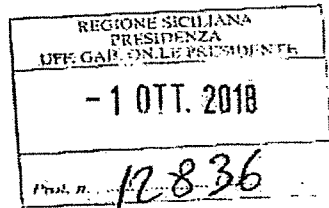
Buona

REPUBBLICA ITALIANA



REGIONE SICILIANA
Responsabile protezione dei dati

20 SET 2018



Prot. n. 51

Palermo, li 28 SET 2018

OGGETTO: Proposta per l'adozione delle prime istruzioni organizzative e tecniche per il trattamento dei dati personali, di una procedura di risposta ad una violazione dei dati personali e di un questionario di autovalutazione.

Al Presidente della Regione

Il Regolamento UE 2016/679 in materia di protezione dei dati, che si applica dal 25 maggio 2018, introduce nuovi diritti degli interessati, nuovi doveri per chi effettua il trattamento di dati e nuovi adempimenti per garantire un corretto ciclo di gestione dei dati delle persone stabilite nell'Unione Europea.

In particolare l'art. 5 par. 2 del Regolamento pone in capo a ciascun titolare dei trattamenti il c.d. principio della responsabilizzazione, in base al quale lo stesso deve assicurare, ed essere in grado di comprovare, il rispetto dei nuovi principi applicabili al trattamento dei dati di cui all'art. 5 par. 1.

Nella consapevolezza che i dati utilizzati posseggono un valore per il soggetto pubblico che li tratta e per i cittadini e che, pertanto, i dati vanno tutelati alla stregua delle altre risorse, economiche, umane ed organizzative, spetta all'Amministrazione regionale l'adozione di una serie di misure tecniche ed organizzative adeguate ed efficaci che traducano il rispetto dei suddetti principi in azioni concrete e in processi amministrativi, e individuino le figure che con il loro operato devono garantire la tutela dei diritti e delle libertà delle persone fisiche.

A tal proposito la S.V. On.le con nota prot. 4329 del 30/3/2018 ha attribuito la competenza organizzativa della materia di che trattasi al dipartimento della Funzione Pubblica e del Personale e con D.P.Reg n. 569 del 12/6/2018, ha nominato del responsabile della protezione dei dati, ai sensi dell'art. 37, attribuendogli i compiti definiti dall'art. 39, tra i quali, informare e fornire consulenza ai titolari e ai responsabili e sorvegliare l'osservanza del Regolamento.

Nell'ambito dei suddetti compiti lo scrivente ha predisposto alcuni documenti che, se adottati dall'Amministrazione, consentono di rendere più efficace l'attività di trattamento dei dati personali svolta negli uffici e dimostrare fattivamente l'impegno profuso dalla Regione Siciliana per garantire il rispetto delle norme o degli standard in materia di protezione dei dati, mediante l'utilizzo di procedure uniformi per tutta l'Amministrazione.

I documenti si inquadrano in un percorso evolutivo dell'Amministrazione che si conforma ai suggerimenti che provengono dal Garante della protezione dei dati personali.

Il primo documento "Prime istruzioni organizzative e tecniche per il trattamento dei dati personali" definisce le politiche interne, uniformi per tutta l'Amministrazione e coerenti con l'attuale quadro legislativo, con riferimento al mutato assetto operativo dell'Amministrazione regionale in tema di protezione dei dati personali.

Vengono riportate le principali figure coinvolte nella gestione dei dati personali (titolari, responsabili, sub-responsabili, sub-responsabili tecnici, referenti privacy, soggetti autorizzati, responsabile della protezione dei dati



e interessati) e vengono declinati dettagliatamente i compiti ad essi attribuiti (gestione dei processi, gestione della sicurezza, supporto ai titolari, gestione dei dati, coordinamento, consulenza, controllo ecc.).

Nel documento, inoltre vengono riportati i procedimenti amministrativi connessi alla protezione dei dati personali, quali il registro delle attività di trattamento tenuti da ciascun titolare del trattamento, il registro delle categorie delle attività di trattamento tenuto da ciascun responsabile, registri delle violazioni, la gestione e l'adeguamento delle informative, la gestione delle violazioni, la cui procedura viene meglio dettagliata nell'apposito documento sotto riportato e il questionario di autovalutazione, al quale si riferisce l'apposito documento riportato nel seguito.

Il secondo documento "Procedura di risposta ad una violazione dei dati personali" definisce le fasi del processo operativo, uniforme per tutta l'Amministrazione, da seguire nel caso si manifesti una violazione di dati personali, descrivendo gli adempimenti a cui sono tenuti i soggetti coinvolti e la sequenza operativa.

In particolare vengono individuati i soggetti che concorrono a garantire che sia inviata la notifica al Garante per la protezione dei dati personali, entro 72 ore dall'accaduto, sulla base degli accertamenti tecnici compiuti dai sub-responsabili tecnici (Sicilia Digitale, ditte esterne ecc.).

Vengono inoltre definite le modalità con le quali si procede ad informare l'interessato affinché possa mettere in atto azioni destinate alla propria cautela.

Il terzo documento "Questionario di autovalutazione sulla conformità al Regolamento UE 679/2016" risponde alla esigenza di monitorare dall'interno dell'Amministrazione il rispetto delle politiche in materia di protezione dei dati personali.

Redatto sulla base di un modello periodicamente rivedibile, il questionario di autovalutazione, va compilato semestralmente a cura di ciascun dipartimento o ufficio equiparato.

Il questionario consente di monitorare il grado di aderenza dell'attività amministrativa alla norma comunitaria, misurando periodicamente gli sviluppi e rilevando le criticità, al fine di porre in essere interventi correttivi.

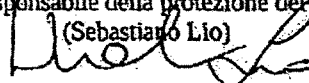
Alla compilazione del questionario provvede ogni Responsabile del trattamento preposto a struttura di massima dimensione, Ufficio di diretta collaborazione, Ufficio alle dirette dipendente o Ufficio Speciale, con il supporto del Referente Privacy, il quale avrà cura di tenere conto adeguatamente dei trattamenti dei dati personali effettuati negli uffici periferici dell'Amministrazione.

Il Dipartimento della Funzione Pubblica e del Personale, ricevuti i questionari, provvederà alla redazione di un report annuale da sottoporre alla Giunta regionale, nel quale siano definiti, di concerto con il Responsabile della protezione dei dati, i principali interventi correttivi.

I suddetti documenti sono stati esaminati ed apprezzati positivamente nella riunione del 27/09/2018 svoltasi presso i locali dell'Ufficio di Gabinetto della S.V. On.le, alla quale hanno partecipato i rappresentanti della Segreteria generale, del dipartimento della Funzione Pubblica e del Personale, dell'Ufficio legislativo e legale, dell'Autorità per l'innovazione tecnologica, oltre allo scrivente, riconoscendo la necessità che gli stessi siano resi operativi nel più breve tempo possibile.

Stante quanto sopra si propongono i documenti di cui sopra affinché, qualora condivisi, siano sottoposti alle valutazioni e alle determinazioni della Giunta regionale, inserendoli nella prima seduta utile.

Il Responsabile della protezione dei dati
(Sebastiano Lio)




IL SEGRETARIO



Principale



Misure attuative del Regolamento 2016/679
del Parlamento Europeo e del Consiglio del 27 aprile 2016

Prime istruzioni organizzative e tecniche per il trattamento dei dati personali

 IL SEGRETARIO
Buon

 Repubblica Italiana  Regione Siciliana	Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 Prime istruzioni organizzative e tecniche per il trattamento dei dati personali
--	--

Il Regolamento UE 2016/679 (Regolamento) interviene sulla tematica già disciplinata sul territorio italiano dal d.lgs. n. 196/2003 c.d. "Codice Privacy", oggi aggiornato dal d.lgs. 101/2018, ed introduce alcuni nuovi principi sulla protezione dei dati personali, nuovi diritti degli interessati, nuovi doveri per chi effettua il trattamento di dati e nuovi adempimenti per garantire un corretto ciclo di gestione dei dati personali.

Ne consegue la necessità di delineare il nuovo assetto operativo dell'Amministrazione regionale in tema di protezione dei dati personali, in relazione alle principali figure dotate di specifiche competenze in materia e ai procedimenti connessi.

Parte A: Figure e competenze


Titolare del trattamento di dati personali

Il Regolamento stabilisce che il Titolare del trattamento (Titolare) è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali". Nella Regione Siciliana, a norma dello Statuto, il Presidente e gli Assessori regionali svolgono le funzioni esecutive ed amministrative e pertanto sono state identificate come titolari dei trattamenti dei dati personali di loro competenza (V. art. 20 dello Statuto della Regione Siciliana, parere dell'Ufficio Legislativo e Legale n. 132 del 2004 e n. 46 del 2005).

I principali compiti del Titolare sono:

- nomina il Responsabile (o i Responsabili) del trattamento con un atto esplicito e gli fornisce le istruzioni sulle modalità di trattamento (art.28);
- mantiene il Registro dei trattamenti svolti sotto la sua responsabilità (art.30);
- mette in atto misure tecniche e organizzative per garantire che il trattamento sia conforme al Regolamento (art.24)
 - effettua le comunicazioni all' Autorità di controllo (in Italia il Garante della protezione dei dati personali) sulla violazione di dati personali (art.33) ed informa l'interessato se si presenta il rischio per i diritti e le libertà di quest'ultimo (art.34) ;
 - tiene un registro delle violazioni dei dati relativi ai trattamenti di propria competenza (art.33);
 - garantisce che i trattamenti siano effettuati in modo lecito, corretto e trasparente e siano adeguati alle finalità (art.5);
 - garantisce che i dati siano esatti, aggiornati, conservati per il tempo strettamente necessario alle finalità e trattati in modo di garantire la loro sicurezza (art.5 e 32);
 - se il trattamento si basa sul consenso dell'interessato, deve poter dimostrare che quest'ultimo lo ha prestato (art. 7);
 - adotta misure appropriate per fornire all'interessato una adeguata informativa sui dati trattati (art. 12);
 - garantisce il diritto d'accesso dell'interessato ai dati che lo riguardano (art. 15), lo informa sui suoi diritti (rettifica o cancellazione dei dati e limitazione o opposizione al loro trattamento) e assicura il corretto godimento dei suoi diritti (artt.15-22);
 - se non è stabilito nell'UE nomina per iscritto un proprio rappresentante nell'Unione (art.27);



 <p>Repubblica Italiana Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Prime istruzioni organizzative e tecniche per il trattamento dei dati personali</p>
--	---

- effettua la valutazione di impatto sui dati personali (DPIA) se si presenta un rischio per le libertà e i diritti personali (art.35);
- designa il Responsabile della protezione dei dati (RPD) (art.37) per Amministrazione regionale e gli fornisce risorse sufficienti per svolgere in modo efficace i suoi compiti (art. 38), per accedere ai dati personali e ai trattamenti e per mantenere la sua conoscenza specialistica;
- si assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali ed in particolare nei processi di definizione di nuovi trattamenti per contribuire alla protezione dei dati sin dalla fase di progettazione e per impostazione predefinita

Responsabile del trattamento dei dati personali


Il Responsabile del trattamento, secondo il Regolamento, è la persona fisica o giuridica, l'amministrazione pubblica o altro organismo che tratta dati personali per conto del Titolare del trattamento. Nella Regione Siciliana i responsabili dei trattamenti vengono di norma individuati nei dirigenti preposti ai dipartimenti, aree e servizi ed unità operative o a posizioni di collaborazione e coordinamento, nonché nei dirigenti preposti agli uffici speciali, agli uffici di diretta collaborazione ed alle dirette dipendenze, in ragione degli incarichi loro conferiti e dei trattamenti effettuati.

L'atto con cui il Titolare designa un Responsabile del trattamento è l'atto esplicito, quale un contratto o di altro atto giuridico equivalente, con il quale gli attribuisce specifici compiti ai sensi del Regolamento e nel quale vengono disciplinati la natura, durata e finalità dei trattamenti assegnati, le 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.

I principali compiti del Responsabile sono:

- tratta i dati per conto del Titolare, sulla base delle istruzioni ricevute (art.28);
- autorizza uno o più soggetti, secondo le esigenze, tra i propri collaboratori, al trattamento dei dati gestiti dalla propria struttura istruendoli nella maniera opportuna;
- garantisce che le persone autorizzate al trattamento dei dati personali siano impegnate nell'assicurare la riservatezza (art.28);
- non ricorre ad altro Responsabile se non autorizzato dal Titolare (art. 28);
- assiste il Titolare con misure tecniche e organizzative adeguate per garantire che questo possa dare seguito alle richieste dell'interessato (art. 28)
- assiste il Titolare nel garantire la sicurezza dei dati personali (art.28);
- mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto degli obblighi di quest'ultimo (art.28);
- mantiene il Registro delle categorie di attività relative ai trattamenti svolti per conto di un Titolare (art.30);
- mette in atto misure tecniche ed organizzative per garantire la sicurezza del trattamento (art.32)
- informa senza ritardo il Titolare in caso di violazione dei dati (art.33) e lo assiste nelle attività conseguenti;
- fornisce risorse sufficienti al RPD per svolgere in modo efficace i suoi compiti (art. 38), accedere ai dati personali e a tutti i trattamenti e per mantenere la propria conoscenza specialistica;
- adotta, se lo ritiene, un codice di condotta approvato a norma dell'art. 40 per dimostrare il rispetto dei suoi obblighi (art.24)



 <p>Repubblica Italiana Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Prime istruzioni organizzative e tecniche per il trattamento dei dati personali</p>
--	---

- coinvolge tempestivamente ed adeguatamente il RPD in tutte le questioni riguardanti la protezione dei dati personali ed in particolare nei processi di definizione di nuovi trattamenti per contribuire alla protezione dei dati sin dalla fase di progettazione e per impostazione predefinita;
- qualora ne ricorrano le condizioni, nomina un Referente Privacy per la propria struttura;

Responsabile della protezione dei dati personali



Il Responsabile della protezione dei dati (RPD o, in inglese, DPO, Data Protection Officer) è una nuova figura istituita dal Regolamento che viene designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti. Svolge le proprie funzioni in autonomia ed indipendenza, senza ricevere istruzioni e in collaborazione diretta con il vertice gerarchico. Con D.P.Reg n. 569 del 12/6/2018 è stato nominato il Responsabile per la protezione di dati dell'Amministrazione regionale in attuazione di quanto deliberato dalla Giunta regionale nella riunione del 23/5/2018.

I compiti del Responsabile della protezione dei dati sono:

- informa e fornisce consulenza al Titolare, al Responsabile ed ai soggetti che trattano i dati (art. 39);
- sorveglia l'osservanza del Regolamento e le politiche adottate dal Titolare e dal Responsabile in materia di trattamenti (art. 39);
- fornisce pareri sulle valutazioni di impatto di cui all'art. 35 del Regolamento (art. 39);
- coopera con l'Autorità di controllo nell'esecuzione dei suoi compiti (artt. 31 e 39)
- funge da punto di contatto con l'Autorità di controllo per facilitarne l'accesso ai documenti ed alle informazioni necessarie (art. 39);
- mantiene il segreto e la riservatezza nell'adempimento dei propri compiti (art. 38).

In particolare il RPD, nell'ambito delle attività di informazione e consulenza e sorveglianza:

- promuove la cultura della protezione dei dati all'interno dell'Amministrazione e contribuisce a dare attuazione agli elementi essenziali del Regolamento;
- predispone i modelli di rilevazione dei dati per i registri di trattamenti per l'intera Amministrazione;
- predispone un modello, uniforme per tutta l'Amministrazione, di richiesta di fruizione dei diritti dell'interessato;
- coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione per la tenuta dei Registri dei trattamenti che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento;
- propone una procedura operativa uniforme di risposta agli incidenti di sicurezza;
- coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione per la tenuta dell'elenco delle Violazioni di dati che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento;
- predispone modelli uniformi di informative per attività svolte da più titolari;
- supporta il Titolare e il Responsabile nelle valutazioni di impatto;
- conduce e supporta audit in materia di protezione dei dati;
- svolge le proprie attività con la collaborazione di un team di dipendenti dotati della necessaria competenza ed incardinati in un ufficio dedicato, posto alle dirette dipendenze del vertice gerarchico dell'Amministrazione. Utilizza per limitati periodi di tempo unità di personale di Sicilia Digitale dotate di specifiche competenze in materia di sicurezza dei dati;

 Repubblica Italiana  Regione Siciliana	Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 Prime istruzioni organizzative e tecniche per il trattamento dei dati personali
--	---

- si avvale del supporto specialistico dell'Ufficio Legislativo e Legale, del Dipartimento Funzione Pubblica e del Personale e dell'Autorità regionale per l'innovazione tecnologica per le materie di rispettiva competenza;
- per le attività di sorveglianza e controllo della sicurezza dei trattamenti di particolare complessità oppure aventi un volume consistente di dati sensibili, il RPD si avvale di soggetti terzi dotati di un livello più elevato di conoscenze specialistiche principalmente di carattere informatico, selezionandoli mediante procedure previste dal codice degli appalti, con il supporto dell'Autorità regionale per l'Innovazione Tecnologica;
- partecipa ai processi di definizione di nuovi trattamenti per contribuire alla protezione dei dati sin dalla fase di progettazione e per impostazione predefinita;
- predispone e mantiene un elenco di domande e risposte comuni (FAQ) sul sito della Regione Siciliana che sia facilmente accessibile ai navigatori.

Referente Privacy

La figura non è prevista dal Regolamento, ma l'art. 2 - quaterdecies, C.1 del D.Lgs.196/2003, modificato dal D.Lgs.101/2018, stabilisce che il Titolare e il Responsabile possano affidare, sotto la propria autorità, specifici compiti e funzioni a figure espressamente designate.

Nelle strutture di massima dimensione, negli Uffici di Gabinetto del Presidente e degli Assessori, negli Uffici speciali, il Responsabile nomina un proprio Referente Privacy con il compito di coordinare l'attuazione delle politiche di protezione dei dati, coadiuvarlo nell'esecuzione dei principali compiti, supportarlo nell'applicazione uniforme delle disposizioni in tema di trattamento dei dati personali.

Inoltre il Referente Privacy supporta il Responsabile nel fornire assistenza al Titolare e nel garantire appropriato e celere riscontro alle richieste del RPD o dell'Autorità di controllo.



Il Referente Privacy deve essere un dipendente dell'Amministrazione dotato di riconosciuta competenza di elevata competenza in materia di protezione dei dati; nel caso di strutture di massima dimensione è incardinato in posizione di Staff. I Referenti Privacy sono coordinati dal dipartimento regionale della Funzione Pubblica e del Personale competente in materia di privacy.

In particolare il Referente Privacy:

- 1) supporta il Responsabile nel tenere aggiornato "Registro delle categorie di attività del Responsabile" (art.30, p.2) e ne dà comunicazione al RPD;
- 2) supporta il Responsabile nel fornire al Titolare l'assistenza necessaria all'aggiornamento del "Registro del Titolare" (art.30, p.1) e ne dà comunicazione al RPD;
- 3) rende conto della propria operatività al Responsabile che lo ha nominato;
- 4) assiste e coordina i soggetti autorizzati al trattamento dei dati nella corretta applicazione del Regolamento;
- 5) supporta il Titolare e il Responsabile in tutte le attività necessarie, conseguenti ad una violazione di dati, curando la predisposizione dell'apposito modello di comunicazione alla Autorità di controllo;
- 6) assiste il Responsabile nell'analisi delle violazioni dei dati compilando e firmando la scheda di rilevazione dati relativa alla violazione.

Soggetti autorizzati al trattamento dati (ex incaricati)

Tali soggetti, individuati dal Responsabile all'interno della propria struttura, trattano i dati personali di competenza della struttura in cui operano, secondo le decisioni e le istruzioni ricevute dal Responsabile e dal sub-Responsabile. In caso di necessità si confrontano con il Referente Privacy e gli forniscono il supporto dallo stesso richiesto.

 Repubblica Italiana  Regione Siciliana	Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 Prime istruzioni organizzative e tecniche per il trattamento dei dati personali
--	--

Sub-Responsabile

Il Responsabile del trattamento può ricorrere ad un altro Responsabile (o ad altri Responsabili) del trattamento, o sub-Responsabile, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, mediante un contratto o un altro atto giuridico con il quale gli siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel contratto tra il Titolare e il Responsabile del trattamento.

Resta fermo che in caso di omissione dell'adempimento degli obblighi suddetti da parte del sub-Responsabile, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-Responsabile.

Nel caso in cui il sub-Responsabile sia incaricato dell'esecuzione di specifiche attività di carattere tecnico (ad es. attività informatiche, centri di contatto con il pubblico, call center, ecc.) assume la denominazione di sub-Responsabile tecnico.

In particolare ciascun Sub-Responsabile in dipendenza delle funzioni affidate:

- gestisce le attività che gli sono state affidate dal Responsabile che lo ha designato;
- cura gli aspetti che garantiscono la corretta gestione e la conservazione dei dati;
- mantiene aggiornati i dati e i sistemi che gli vengono affidati badando alla loro manutenzione ed alla loro protezione;
- garantisce la collaborazione e il supporto al Responsabile ed al Titolare per tutte le operazioni che riguardano le attività affidate;
- garantisce la collaborazione e il supporto nelle verifiche tecniche, svolte dai soggetti individuati dal Titolare, dal Responsabile o dal RPD, tese ad accertare la sicurezza dei dati, dei sistemi e la correttezza del trattamento.

sub-Responsabile tecnico

Il Responsabile del trattamento può ricorrere ad un sub-Responsabile tecnico per l'esecuzione di specifiche attività di carattere tecnico (ad es. attività informatiche, centri di contatto con il pubblico, call center, ecc.)

Per l'aspetto informatico questo ruolo estremamente importante viene svolto dalle società partecipate (Sicilia Digitale, SEUS 118 ecc.) o da ditte esterne selezionate con regolari processi di acquisto, sulla base delle indicazioni, linee guida e coordinamento dell'Autorità regionale per l'Innovazione Tecnologica.

In particolare ciascun Sub-Responsabile tecnico in dipendenza delle funzioni affidate:



- gestisce le attività tecniche che gli sono state affidate dal Responsabile che lo ha designato;
- cura gli aspetti tecnici che garantiscono la corretta gestione e la conservazione dei dati;
- mantiene in efficienza la rete di trasmissione dati badando alla sua manutenzione ed alla sua protezione, qualora gli sia stata affidata;
- garantisce la collaborazione e il supporto al Responsabile ed al Titolare per tutte le operazioni che riguardano le attività affidate;
- garantisce la collaborazione e il supporto nelle verifiche tecniche, svolte dai soggetti individuati dal Titolare, dal Responsabile o dal RPD, tese ad accertare la sicurezza dei dati, dei sistemi e la correttezza del trattamento.

Interessati

Il Regolamento definisce "interessato" una persona fisica vivente, identificata o identificabile e stabilita nell'Unione Europea. L'identificazione può avvenire direttamente o indirettamente, ad es. con il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo online, uno



Buon

 Repubblica Italiana  Regione Siciliana	Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 Prime istruzioni organizzative e tecniche per il trattamento dei dati personali
--	--

o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Online le persone fisiche possono essere identificate tramite dispositivi, applicazioni, strumenti e protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o a identificativi di altro tipo.

I diritti degli interessati tutelati dal Regolamento sono:

- diritto all'accesso ai dati, ovvero ad ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento di dati personali che lo riguardano e in tal caso ottenere le informazioni specificate nell'art.15;
- diritto alla rettifica dei dati previsto dall'art. 16;
- diritto alla cancellazione o all'oblio previsto dall'art.17;
- diritto alla limitazione del trattamento previsto all'art.18;
- diritto alla portabilità dei dati, ovvero a ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i propri dati personali e a trasmetterli a un altro Titolare, previsto dall'art. 20;
- diritto di opposizione al trattamento (art.21)
- diritto al risarcimento (art.82).

Le modalità per l'esercizio dei diritti sono dettagliatamente disciplinate dall'art. 12 del Regolamento. Di regola l'interessato effettua una richiesta che il Titolare riscontra senza ingiustificato ritardo e comunque entro un mese. In presenza di un elevato numero di richieste o di complessità della richiesta il termine può essere prorogato di 2 mesi informando l'interessato.

Autorità di controllo

Il Regolamento definisce Autorità di controllo "l'autorità pubblica indipendente istituita da uno Stato membro" della Unione Europea, incaricata di sorvegliare l'applicazione del regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione.

Nella Repubblica Italiana il ruolo è svolto dal Garante della protezione dei dati personali (Garante).


I principali compiti del Garante sono dettagliati negli artt. 55 e seguenti del Regolamento e riguardano la sorveglianza sull'applicazione del Regolamento nel territorio italiano, le attività di indagine in merito, la trattazione dei reclami proposti da un interessato e la promozione della consapevolezza e della corretta comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento.

Parte B: Procedimenti

Trattamento dei dati personali

Il Regolamento definisce come Trattamento "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di 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". Quindi un Trattamento è qualunque operazione compiuta sui dati personali personali di un soggetto, quali ad esempio il ricevimento di una istanza contenente dati personali, la gestione di tali dati, la firma di un atto o di un decreto contenente dati personali, la gestione di un archivio, l'estrazione dei dati di un archivio,



 <p>Repubblica Italiana Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Prime istruzioni organizzative e tecniche per il trattamento dei dati personali</p>
--	---

la sua pubblicazione ecc. Il Trattamento può riguardare, ad esempio, la gestione di contributi o pagamenti che riguardino persone fisiche, la gestione del processo di acquisto di beni o servizi, la gestione del personale, la gestione di archivi riguardanti la salute dei cittadini (inclusi i dati sensibili, sanitari, biometrici, genetici ecc.), la videoregistrazione, la gestione del contenzioso, la gestione di servizi web rivolti al pubblico, la gestione di sistemi di posta elettronica, la memorizzazione di indirizzi IP o indirizzi MAC ecc.

Vale la pena di precisare che i dati personali sono qualunque informazione riguardante una persona fisica identificata o identificabile, ad es. il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Non si possono considerare dati personali le informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il Regolamento non si applica pertanto al trattamento di informazioni anonime, anche per finalità statistiche o di ricerca.

Registro delle attività di trattamento e delle categorie delle attività

Tra i nuovi adempimenti del Regolamento vi è anche l'istituzione e la tenuta dei Registri delle attività di trattamento a cura del Titolare del trattamento (art. 30 co. 1) e dei Registri delle categorie di attività di trattamento a cura del Responsabile del trattamento (art. 30 co. 2) in forma scritta, anche elettronica, da mettere a disposizione dell'Autorità di controllo, su richiesta.

I Registri, quindi, sono almeno due, uno tenuto dal Titolare e uno da ciascun Responsabile, ma redatti ed aggiornati in sintonia. I contenuti dei Registri sono descritti dettagliatamente nel suddetto articolo del Regolamento e riguardano, tra l'altro, i dati nominativi e di contatto, del Titolare e del Responsabile, del RPD, le finalità del trattamento, le categorie di dati trattati e dei soggetti interessati, gli eventuali destinatari a cui i dati saranno comunicati ed eventuali trasferimenti degli stessi verso paesi non appartenenti alla UE, la durata del trattamento e i termini per la cancellazione dei dati, nonché le misure di sicurezza di carattere organizzativo e tecnico messe in atto per garantire, tra l'altro, la riservatezza, l'integrità, la non divulgazione dei dati e l'accesso controllato e rispettoso delle finalità del trattamento. Nulla vieta a un Titolare o un Responsabile di inserire ulteriori informazioni qualora lo ritenga opportuno, nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Se designato, il Referente Privacy supporta il Titolare o il Responsabile nell'aggiornamento del registro di sua competenza.


La scadenza per la predisposizione del registro tenuto dal Titolare e del registro tenuto dal Responsabile è il 25/5/2018, data di inizio applicazione del Regolamento.

Il Titolare ed il Responsabile provvedono all'aggiornamento del proprio registro ogni volta che se ne presenti l'esigenza e comunque almeno ogni trimestre.

Al di là dell'adempimento formale la tenuta dei registri dei trattamenti costituisce un elemento fondamentale per la corretta gestione dei dati personali, necessario per disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Amministrazione ed indispensabile per ogni valutazione e analisi del rischio per i diritti e le libertà delle persone fisiche che il Regolamento tutela.

Per garantire l'uniformità delle informazioni raccolte dai Titolari e dai Responsabili, il RPD predispone i modelli di rilevazione dei dati per i registri di trattamenti per l'intera Amministrazione regionale, che vengono aggiornati dal Titolare e dal Responsabile almeno ogni trimestre.



 <p>Repubblica Italiana Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Prime istruzioni organizzative e tecniche per il trattamento dei dati personali</p>
--	---

Il RPD inoltre coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione per la tenuta dei Registri dei trattamenti che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento da parte del Titolare e del Responsabile.

Violazioni dei dati personali (Data Breach)

La violazione dei dati si manifesta quando avviene una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Responsabile per conto del Titolare.

Il Regolamento stabilisce che il Titolare effettua le comunicazioni all'Autorità di controllo sulla violazione di dati personali (art.33) ed informa l'interessato se si presenta il rischio per i diritti e le libertà di quest'ultimo (art.34).

Il modello che viene utilizzato è quello messo a disposizione dal Garante, che è disponibile nel sito di quest'ultimo.

Il modello va compilato dal Titolare, assistito dal Responsabile del trattamento e con l'ausilio del Referente Privacy, sulla base delle informazioni fornite dal sub-Responsabile e dal sub-Responsabile tecnico che cura la gestione informatizzata dei dati e quindi notificato all'Autorità di controllo da parte del Titolare.

Inoltre il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze in cui è avvenuto, le conseguenze ed i provvedimenti adottati per porvi rimedio (art.33); per tali fini ciascun Titolare tiene un registro delle violazioni dei dati, che include le violazioni avvenute presso il Responsabile, il sub-Responsabile e il sub-Responsabile tecnico coinvolti nei trattamenti di dati personali del Titolare.

Al fine di catalogare unitariamente le violazioni il RPD coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione per la tenuta dell'elenco delle Violazioni di dati che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento.

Inoltre al fine di rendere il più possibile omogenee le procedure seguite nell'Amministrazione regionale nei casi di violazioni di dati, il RPD propone una procedura operativa di risposta agli incidenti di sicurezza.

Informativa all'interessato

Il Titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento (art. 13 - 22 e 34).


L'informativa va resa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informative sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Non è necessario fornire l'informativa se l'interessato ne dispone già, se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiede uno sforzo sproporzionato.

Le principali informazioni da fornire agli interessati sono diverse nel caso in cui vengono raccolte presso l'interessato, ad es. tramite siti web, (art. 13) o da altre fonti (art.14).

La informativa viene predisposta dal Titolare, assistito dal Responsabile, dal sub-Responsabile e con il supporto del Referente Privacy, sulla base del trattamento effettuato. Al fine di rendere

<p>Repubblica Italiana</p>  <p>Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Prime istruzioni organizzative e tecniche per il trattamento dei dati personali</p>
---	---

omogenee le informative rese dai rami dell'Amministrazione il RPD predisporrà modelli di informative da utilizzarsi per attività di interesse da parte più Titolari.

Questionario di Autovalutazione

Al fine di monitorare dall'interno il rispetto delle *policy* in materia di protezione dei dati personali viene adottato, sulla base del modello proposto dal RPD aggiornabile all'occorrenza, un questionario di autovalutazione, da compilarsi semestralmente a cura di ciascun dipartimento o ufficio equiparato.

Il questionario consente di monitorare il grado di aderenza dell'attività amministrativa alla norma comunitaria, misurando periodicamente gli sviluppi e rilevando le criticità, al fine di porre in essere interventi correttivi.

Alla compilazione del questionario provvede ogni Responsabile preposto a struttura di massima dimensione, Ufficio di diretta collaborazione, Ufficio alle dirette dipendente o Ufficio Speciale, con il supporto del Referente Privacy, il quale avrà cura di tenere conto adeguatamente dei trattamenti dei dati personali effettuati negli uffici periferici dell'Amministrazione.

Il Dipartimento della Funzione Pubblica e del Personale, ricevuti i questionari, provvederà alla redazione di un report annuale da sottoporre alla Giunta regionale, nel quale siano definiti, di concerto con il RPD, i principali interventi correttivi.



Buon




Misure attuative del Regolamento 2016/679
del Parlamento Europeo e del Consiglio del 27 aprile 2016

Procedura di risposta ad una violazione dei dati personali



IL SEGRETARIO

[Handwritten signature]

<p>Repubblica Italiana</p>  <p>Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Procedura di risposta ad una violazione dei dati personali</p>
---	--

1. Generalità

Il Regolamento UE 2016/679 stabilisce che si manifesta una violazione dei dati personali (*data breach*) quando avviene una violazione di sicurezza che determina, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Responsabile per conto del Titolare, che comporti un rischio per i diritti e le libertà delle persone fisiche.

Rientrano nella fattispecie gli eventi e i comportamenti atti a danneggiare i dati, a comprometterne la disponibilità o l'integrità indipendentemente da finalità o interventi fraudolenti, nonché gli incidenti avvenuti per fatti accidentali che compromettono l'integrità dei dati.

Fatti simili si verificano nella gestione e conservazione di dati con supporti informatici e tecnologici, ma assumono rilevanza per l'art. 33 del Regolamento UE 2016/679 quando la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

La corretta gestione del *data breach* ed in particolare la valutazione degli aspetti di rilevanza giuridica, organizzativa, tecnica e tecnologica, nonché quelli inerenti gli interventi posti in essere hanno una notevole rilevanza per limitare le conseguenze sui diritti e le libertà personali degli interessati e per prevenire o evitare eventuali conseguenze di carattere economico-finanziarie dovute a pretese risarcitorie e danni per l'Amministrazione regionale.

2. La violazione di sicurezza

Il Gruppo di lavoro articolo 29, istituito dall'Unione Europea, ha individuato nelle sue linee guida del 6/2/2018 in materia di *data breach*, tre categorie di eventi rilevanti ai sensi degli artt. 33 e 34 del Regolamento:

- quando vi è un accesso incidentale o abusivo a dati personali;
- quando vi è una perdita o distruzione accidentale o non autorizzata del dato personale;
- quando vi è un'alterazione accidentale o non autorizzata del dato personale.

Nel caso concreto la violazione può riguardare anche più di una di queste categorie.

Per valutare la presenza di un rischio per i diritti e le libertà delle persone fisiche evidenzia, vanno considerati i seguenti elementi:

- il tipo di violazione;
- la natura, il numero e il grado di sensibilità dei dati personali violati;
- la facilità di associare i dati violati a una persona fisica;
- la gravità delle conseguenze per gli interessati;
- il numero di interessati esposti al rischio;
- le caratteristiche del titolare del trattamento come, per esempio, le dimensioni dell'ente, il tipo di attività svolta, la qualità e quantità di dati trattati.

3. La notifica al Garante della protezione dei dati personali

Il Regolamento stabilisce che il Titolare effettua le comunicazioni al Garante della protezione dei dati personali (Garante) sulla violazione di dati personali (art. 33) ed informa l'interessato se si presenta il rischio per i diritti e le libertà di quest'ultimo (art. 34).


Lo stesso articolo prevede che la notifica non sia necessaria laddove sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

4. Il Modello di notifica

Il modello che viene utilizzato è quello messo a disposizione dal Garante, disponibile anche nel sito della Regione Siciliana nella sezione del RPD.

Il modello da trasmettere al Garante:



<p>Repubblica Italiana</p>  <p>Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Procedura di risposta ad una violazione dei dati personali</p>
---	--

- descrive la natura della violazione dei dati personali
- descrive le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunica il nome e i dati di contatto del Responsabile della protezione dei dati e di altro punto di contatto presso cui ottenere più informazioni;
- descrive le probabili conseguenze della violazione dei dati personali;
- descrive 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.

5. La compilazione del Modello

Il modello va compilato dal Responsabile del trattamento con il supporto del sub-Responsabile e del Referente Privacy e avendo consultato il sub-Responsabile tecnico che cura la gestione informatizzata dei dati e viene quindi inviato al Titolare perché lo faccia proprio e provveda all'inoltro al Garante entro 72 ore dal momento in cui la violazione è conosciuta. Entro questo termine il Titolare deve essere in grado di identificare la violazione, revisionare eventuale documentazione, adottare procedure e/o atti che mitigano il danno arrecato e notificare il *data breach* al Garante.

6. La comunicazione all'interessato

L'art. 34 del Regolamento stabilisce che quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento debba comunicare la violazione all'interessato senza ingiustificato ritardo. Ciò al fine di consentire all'interessato di proteggersi da eventuali conseguenze dannose derivanti dal *data breach*.

La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure di cui all'art. 33, paragrafo 3, lettere b), c) e d).

Il Titolare è esonerato dal comunicare il *data breach* all'interessato nel caso in cui:

- siano state implementate misure di sicurezza adeguate e tali misure erano già state applicate ai dati personali oggetto del *data breach* (per esempio la cifratura);
- dopo il *data breach* sono state adottate misure di sicurezza atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione all'interessato richiederebbe sforzi sproporzionati e quindi si può procedere a una comunicazione pubblica.

7. Il Registro delle Violazioni

Inoltre il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze in cui è avvenuto, le conseguenze ed i provvedimenti adottati per porvi rimedio (art.33); per tali fini ciascun Titolare tiene un registro delle violazioni dei dati, che include le violazioni avvenute presso i Responsabili, i sub-Responsabili e i sub-Responsabili tecnici coinvolti nei trattamenti di dati personali di ciascun Titolare.


Il Registro potrà essere esaminato dal Garante per verificare il rispetto delle norme in materia.

Il Registro deve riportare:

- le circostanze relative a qualsiasi violazione dei dati personali e le sue conseguenze;
- i provvedimenti adottati per porvi rimedio.

Inoltre il Titolare deve motivare le decisioni assunte, riportandole nel Registro, in particolare nel caso in cui abbia deciso di non procedere alla notifica, oppure abbia ritardato nella procedura di notifica, oppure abbia deciso di non comunicare il *data breach* agli interessati.




 <p>Repubblica Italiana Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Procedura di risposta ad una violazione dei dati personali</p>
--	--

Al fine di catalogare unitariamente le violazioni il RPD coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione regionale per la tenuta dell'elenco delle Violazioni di dati che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento. La documentazione delle violazioni avvenute consente al Titolare, assistito dal Responsabile, di aggiornare regolarmente i processi per adottare tutte le misure tecniche e organizzative più appropriate, alla luce delle criticità evidenziate dagli eventi accaduti.

8. La procedura in caso di *data breach*

La procedura di *data breach* si articola nelle seguenti fasi:

- a) comunicazione del fatto: il soggetto che venga a conoscenza di un fatto o di una circostanza che determini o possa determinare una violazione dei dati personali informa, senza ingiustificato ritardo, il Titolare del trattamento, il Responsabile del trattamento, il sub-Responsabile, il sub-Responsabile tecnico, il Referente Privacy e il RPD inviando una segnalazione per posta elettronica o telefonica. Qualora la segnalazione sia effettuata da un interessato e pervenga ad un solo dei soggetti sopra elencati, questi provvede ad informarne gli altri;
- b) accertamento della violazione: il Referente Privacy, supportato dal sub-Responsabile e, nel caso di dati informatizzati, dal sub-Responsabile tecnico, acquisisce le informazioni sulla segnalazione, sul contesto, sugli effetti della violazione e ogni ulteriore informazione utile all'accertamento della violazione;
- c) valutazione della violazione: il Referente Privacy, supportato dal sub-Responsabile e, nel caso di dati informatizzati, dal Sub-Responsabile tecnico effettua una prima valutazione sul fatto descritto in base degli elementi acquisiti, sul rischio per i diritti e le libertà delle persone fisiche interessate. Qualora si possa considerare ragionevolmente certo che il rischio per i diritti e le libertà delle persone fisiche non sia elevato, comunica in forma scritta al Responsabile, al Titolare e al RPD la valutazione e procede alla semplice registrazione dell'evento nel Registro delle violazioni.
- d) comunicazione al Garante: qualora non possa considerarsi ragionevolmente certo un rischio significativo per i diritti e le libertà dell'interessato, il Referente Privacy supportato dal sub-Responsabile e, nel caso di dati informatizzati dal sub-Responsabile tecnico, predispone il modello di notifica della violazione al Garante, lo consegna al Responsabile per la sua trasmissione al Titolare, affinché quest'ultimo possa procedere alla notifica senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Se non è rispettato il termine delle 72 ore, il ritardo dev'essere giustificato adducendo una adeguata motivazione. La notifica è effettuata con nota protocollata, inviata tramite PEC. Copia del modello e degli altri atti connessi viene conservato agli atti ed anche inviato al RPD;
- e) comunicazione all'interessato: il Titolare, assistito dal Responsabile e con il supporto del Referente Privacy, del sub-Responsabile e del Sub-Responsabile tecnico, comunica la violazione all'interessato senza ingiustificato ritardo e in maniera chiara e trasparente, tramite l'invio di una mail o, in mancanza, altra forma di comunicazione (per es. telefonica o cartacea). Nel caso in cui ci siano più interessati e la comunicazione diretta richiederebbe sforzi ingenti si procede a una comunicazione pubblica, o misura simile, tramite la quale gli interessati sono informati con analogo efficacia, per es. pubblicazione di un avviso evidente nella home page del portale istituzionale per un congruo numero di giorni oppure notifica sempre tramite il portale istituzionale (art. 34).
- f) il Responsabile con il supporto del Referente Privacy, del sub-Responsabile e, ove presente il sub-Responsabile tecnico, dispone quanto necessario affinché si provveda con urgenza ai

<p>Repubblica Italiana</p>  <p>Regione Siciliana</p>	<p>Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016</p> <p>Procedura di risposta ad una violazione dei dati personali</p>
---	--

primi adempimenti per limitare le conseguenze dell'evento e per evitare il ripetersi a breve termine dell'evento. Di ciò informa il RPD;

- g) compilazione del registro: il Titolare del trattamento, assistito dal Responsabile e con il supporto del Referente Privacy documenta i fatti nel registro delle violazioni, ed in particolare le circostanze relative a qualsiasi violazione dei dati personali le sue conseguenze, i provvedimenti adottati per porvi rimedio e la motivazione delle decisioni assunte, in particolare nel caso in cui abbia deciso di non procedere alla notifica, ed eventuali ritardi con le rispettive cause.
- h) il Titolare, assistito dal Responsabile, con il supporto del Referente Privacy, del sub-Responsabile e del Sub-Responsabile tecnico effettua una valutazione di opportunità sul procedere ad una approfondita Valutazione di impatto sui dati personali sul trattamento interessato dalla violazione e in merito consulta il RPD;
- i) il Titolare, assistito dal Responsabile, con il supporto del Referente Privacy, del sub-Responsabile e del sub-Responsabile tecnico mette in atto tutti i provvedimenti definitivi ritenuti necessari anche sulla scorta degli esiti dell'eventuale Valutazione di impatto condotta. Di ciò informa il RPD.

Esempi di Violazioni di sicurezza

Si riportano nel seguito alcuni esempi di violazioni di sicurezza:

- un attacco informatico ad uno o più sistemi informativi
- la distruzione o perdita di dati per cause differenti da un attacco informatico o da problemi tecnici;
- un'interruzione del servizio di un sistema di gestione dati dell'Amministrazione causato ad esempio da una interruzione di energia elettrica, che rende i dati personali non più disponibili;
- la impossibilità di accedere a dati crittografati qualora sia andata persa la chiave di decrittografia;
- il furto o smarrimento di un computer portatile, di un cellulare di servizio non opportunamente cifrato;
- lo smarrimento di una chiavetta USB che contiene dati personali di dipendenti o cittadini.



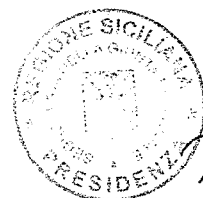
Repubblica Italiana




Regione Siciliana

**Misure attuative del Regolamento 2016/679
del Parlamento Europeo e del Consiglio del 27 aprile 2016**

**Questionario di autovalutazione
sulla conformità al Regolamento UE 679/2019
sulla protezione dei dati personali**




 Repubblica Italiana Regione Siciliana	Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 Questionario di autovalutazione sulla conformità al Regolamento UE 679/2019 sulla protezione dei dati personali
---	--

Dipartimento _____		Anno _____		
Semestre _____		Anno _____		
Quèsti	Valutazione			Precisioni e approfondimenti
	Raggiunto	Parzialmente raggiunto	Non raggiunto	
1	I trattamenti di categorie particolari di dati, che possono rivelare l'origine razziale ed etnica, convinzioni religiose, filosofiche, ecc., opinioni politiche, adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, stato di salute e vita sessuale, vengono effettuati garantendo un elevato grado di sicurezza per i diritti e le libertà personali?			
2	Le informative sono state integrate con le informazioni di cui all'art.13 e 14 Regolamento UE 679/2016? (Le informative devono contenere ulteriori informazioni rispetto a quelle contemplate nel D.Lgs.196/2003 ad es. tempo di conservazione dei dati, base giuridica del trattamento, legittimo interesse del titolare, etc.).			
3	Per i trattamenti che vengono effettuati sulla base del consenso rilasciato dagli interessati qual'è il grado di aderenza all'art. 7 del Regolamento? Ai sensi dell'art.7 del Regolamento, se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Il consenso è revocato con la stessa facilità con cui è accordato. Il titolare deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso			
4	Viene aggiornato periodicamente il registro delle attività di trattamento del Titolare? Art.30 c.1 Regolamento. (Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità)			
5	Viene aggiornato periodicamente il registro delle categorie di trattamento di trattamento del Responsabile? Art.30 c.2 Regolamento (Ogni responsabile del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità)			
6	I Responsabili sono stati designati con atto esplicito da parte del Titolare? Art. 28 Regolamento Il Titolare designa un Responsabile del trattamento con un atto esplicito, quale un contratto o di altro atto giuridico equivalente, con il quale gli attribuisce specifici compiti ai sensi del Regolamento e nel quale vengono disciplinati la natura, durata e finalità dei trattamenti assegnati, le 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.			



[Handwritten signature]

 Repubblica Italiana Regione Siciliana	Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 Questionario di autovalutazione sulla conformità al Regolamento UE 679/2019 sulla protezione dei dati personali
---	--

7 I soggetti che sono autorizzati al trattamento sono istruiti in tal senso dal Responsabile? Art.32 Comma 4 Regolamento Il titolare dei dati deve aumentare la sensibilizzazione e fornire la formazione a tutti i soggetti coinvolti nel trattamento dei dati personali.					
8 I dipendenti hanno partecipato effettivamente a corsi o incontri sulla protezione dei dati personali?					
9 E' stata definita una procedura interna di gestione dei reclami degli interessati che definisca un iter operativo compatibile con i tempi massimi per il riscontro?					
10 Sono state messe in atto misure tecniche per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? Art.32 Regolamento					
11 Le procedure relative al backup dei dati, al ripristino e ai test di ripristino sono adeguatamente documentate? Art.32 Regolamento					
12 Esistono procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento? Art.32 Regolamento					
13 Si sta predisponendo la procedura per la realizzazione della valutazione di impatto? (PIA) Art.35 Regolamento 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.					
14 Si sono verificate violazioni di dati personali nel semestre? (Data Breach)					
15 Sono state notificate violazioni di dati personali al Garante per la protezione dei dati personali? Art.33 Regolamento In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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					
16 Nelle questioni riguardanti la protezione dei dati personali ed in particolare nei processi di definizione di nuovi trattamenti per contribuire alla protezione dei dati sin dalla fase di progettazione e per impostazione predefinita è stato coinvolto il Responsabile protezione dei dati?					
Il Referente Privacy	Il Dirigente Generale				
_____	_____				

