LINEE GUIDA PER LA NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH*) PER GLI UFFICI DELL'AGENZIA REGIONALE PER LO SVILUPPO RURALE – ERSA

1. Premessa

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, noto anche come *General data protection regulation* (di seguito GDPR), in vigore dal 24 maggio 2016 e pienamente applicabile dal 25 maggio 2018, è stato adottato dagli organi comunitari con la finalità di garantire un livello di tutela equivalente per i dati personali in tutto il territorio dell'Unione Europea, superando in tal modo la precedente frammentazione normativa.

A differenza della Direttiva 95/46/CE, esso è direttamente applicabile nei Paesi membri senza necessità di un atto di recepimento ed ha lo scopo di creare un quadro normativo più coerente ed omogeneo per far fronte alla rapidità dell'evoluzione tecnologica e alla globalizzazione, che hanno aumentato notevolmente la portata della raccolta, della condivisione e della circolazione dei dati con strumenti informatici e telematici.

Tra gli aspetti più rilevanti del nuovo quadro normativo, rientra anche l'obbligo di definire una procedura da porre in essere in caso di *data breach*, ovvero di violazione dei dati personali.

Il GDPR detta la normativa di riferimento per la disciplina di tale fattispecie rispettivamente nei Considerando C85, C86, C87, C88 e negli articoli 4, paragrafo 1, n. 12), 33 e 34. Ulteriori disposizioni sono contenute inoltre nelle linee guida del Gruppo di lavoro Art. 29 (*Guidelines on Personal data breach notification under Regulation 2016/679*), adottate il 3 ottobre 2017 e s.m.i..

2. Data breach

a. definizione

La violazione di dati personali (*data breach*) è un particolare tipo di incidente di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati, che può compromettere la riservatezza, l'integrità o la disponibilità dei dati medesimi.

Le diverse tipologie di violazioni di dati personali prese in considerazione nella fattispecie in esame possono essere classificate come segue:
- violazione della riservatezza, intesa come divulgazione o accesso non autorizzati o accidentali;
- violazione dell'integrità, consistente in una modifica non autorizzata o accidentale;
- violazione della disponibilità, in caso di perdita o distruzione non autorizzate o accidentali.

b. esempi

Costituiscono casi di violazione, a titolo meramente esemplificativo, eventi quali:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- lo smarrimento di documenti;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, quali virus, *malware*, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;

- la perdita, la distruzione o la cancellazione per errore di documenti contenenti dati personali, senza avere il possesso di un'eventuale copia;
- la divulgazione non autorizzata dei dati personali, quali ad esempio la pubblicazione sul sito di dati personali al di fuori dei casi previsti dalla legge;
- la comunicazione, per errore, di dati personali a soggetti diversi dal destinatario.

3. Gestione del data breach

Gli obblighi nascenti dalla vigente normativa in caso si verifichi un *data breach*, al ricorrere dei presupposti espressamente previsti, sono i seguenti:
a) obbligo di notifica al Garante per la protezione dei dati personali;
b) obbligo di comunicazione agli interessati;
c) obbligo di documentare le violazioni in un apposito Registro.

a. obbligo di notifica al Garante entro 72 ore

All'articolo 33 il GDPR prevede espressamente che, in caso di violazione dei dati personali, il Titolare del trattamento deve notificare la violazione all'autorità di controllo competente – il Garante per la protezione dei dati personali - senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che tale violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica ha la funzione di consentire all'Autorità di applicare le misure correttive a sua disposizione previste dall'articolo 58 del GDPR e di adottare misure di tutela immediate a favore dei soggetti coinvolti.

Il Titolare del trattamento è quindi chiamato ad effettuare, in tempi molto ristretti, una valutazione sulla gravità dell'impatto della violazione sui diritti e sulle libertà delle persone fisiche. La tempestività è un elemento centrale della procedura di notificazione, conseguentemente viene fissato un termine molto breve per la sua effettuazione.

E' essenziale a tal fine che sia dimostrabile il momento dell'avvenuta conoscenza della violazione, poiché da quel momento decorre il termine per la notifica. Qualora tale termine non venga rispettato, la notifica dovrà essere accompagnata dalla descrizione dei motivi del ritardo.

b. obbligo di comunicazione agli interessati

Se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve effettuare la comunicazione dell'evento anche a tutti gli interessati, senza "ingiustificato ritardo" ed utilizzando i canali più idonei. Con la notifica questi soggetti sono posti nella condizione di attivarsi direttamente per la tutela dei propri interessi.

Non è richiesta la comunicazione all'interessato, se è soddisfatta una delle seguenti condizioni:
- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure sono state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione agli interessati richiederebbe sforzi sproporzionati, nel qual caso si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

c. tenuta del Registro delle violazioni

Il Titolare del trattamento, a prescindere dalla notifica al Garante, è chiamato in ogni caso a documentare tutte le violazioni dei dati personali, predisponendo un apposito **Registro delle violazioni**, al fine di consentire al Garante di verificare il rispetto della normativa.

Pertanto tutte le attività di scoperta e trattamento degli incidenti di tale natura dovranno essere documentate e tracciabili in un apposito Registro detenuto presso la Segreteria del Direttore generale, in modo da fornire evidenza dei fatti e delle operazioni effettuate, anche nel caso in cui non siano seguite dalle notifiche e comunicazioni previste dalla legge.

4. Soggetti coinvolti nelle procedure di notifica

La responsabilità di gestire il processo generale degli incidenti di sicurezza è affidata al **Titolare del trattamento**, nella persona del Direttore generale dell'ERSA, il quale ha il compito di notificare il *data breach* al Garante per la protezione dei dati personali e, laddove necessario, comunicare la violazione agli interessati nel rispetto dei termini previsti.

I **Direttori di Servizio** hanno l'obbligo di segnalare al Titolare del trattamento il potenziale *data breach*, qualora rilevino nel proprio contesto organizzativo, su segnalazione interna (personale del proprio Servizio) o su segnalazione di terzi, la presenza di una possibile violazione dei dati personali presenti sia nei sistemi informativi che nella documentazione cartacea. Hanno altresì l'obbligo di collaborare con il Titolare nella gestione della procedura, fornendo ogni elemento di valutazione ritenuto necessario o utile.

In tale contesto la figura del ***Responsabile della protezione dei dati – RPD,*** di cui all'articolo 37 e seguenti del GDPR, si configura come consulente per il Titolare nell'attuazione di tutti gli adempimenti necessari, ma anche come punto di riferimento per i soggetti interessati.

5. Modalità di svolgimento delle procedure di notifica e comunicazione

Nella definizione delle procedure di notifica e comunicazione, vanno distinte due diverse casistiche, le quali comportano una diversa gestione del *data breach*, come di seguito identificate;
a) trattamenti di dati gestiti direttamente dall'ERSA;
b) trattamenti di dati affidati a Responsabili esterni all'ERSA.

a. trattamenti gestiti direttamente dall'ERSA

A seguito della scoperta o della ricezione di una comunicazione di *data breach*, il Titolare del trattamento è chiamato ad effettuare una breve istruttoria per valutare se sussistano i presupposti per la notifica al Garante, tenendo conto della gravità dell'impatto della violazione intercorsa sui diritti e sulle libertà delle persone fisiche. Nella valutazione del caso è supportato dal Direttore del Servizio competente e dal Responsabile della protezione dei dati.

Qualora, in esito a tale valutazione, si ritenga non sussistente l'esigenza di notifica al Garante, la procedura termina con l'archiviazione del caso e la sua annotazione nel Registro delle violazioni.

Nel caso in cui il Titolare concluda invece l'istruttoria ritenendo necessaria la notifica al Garante, procederà nel **termine di 72 ore** tramite PEC, specificando nella stessa le seguenti informazioni:
a) natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolte dalla violazione;
b) nome e dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) probabili conseguenze della violazione dei dati personali;
d) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

In caso di violazioni complesse il Titolare può valutare di eseguire la notifica al Garante per fasi, completando la procedura dopo le 72 ore. In tal caso dovrà avviare comunque una prima notifica entro le 72 ore, nella quale specificherà e motiverà l'esigenza di fornire ulteriori dettagli in un momento successivo.

Il Titolare del trattamento, coadiuvato dal RPD e dal dirigente responsabile della struttura presso cui si è registrata la violazione dei dati, effettua quindi successivamente una breve istruttoria per valutare se comunicare la violazione anche agli interessati, ai sensi dell'articolo 34 del GDPR.

Qualora in esito all'istruttoria venga rilevata la necessità di avvisare gli interessati, la relativa comunicazione dovrà contenere le seguenti informazioni minime:
- descrizione della natura della violazione;
- nome e dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia.

Se viceversa l'istruttoria si conclude definendo la non necessità di comunicare la violazione all'interessato, è comunque possibile che il Garante, ai sensi dell'articolo 34, paragrafo 4, richieda che tale comunicazione venga effettuata, qualora ritenga che la violazione possa presentare un rischio elevato per i suoi diritti.

Il Titolare del trattamento, con la cooperazione del dirigente del Servizio ove si è verificata la violazione, provvede ad applicare tutte le misure necessarie per arginare i possibili danni conseguenti alla violazione. Inoltre valuta eventuali misure future necessarie per evitare il ripetersi dell'evento dannoso.

L'Ente provvede a documentare tutte le azioni intraprese e ad aggiornare il Registro delle violazioni di cui in premessa.

b. trattamenti affidati a Responsabili esterni all'ERSA

Il Responsabile del trattamento svolge un ruolo importante nel consentire al Titolare di adempiere tempestivamente agli obblighi in materia di *data breach*. Pertanto è essenziale che il contratto che disciplina i rapporti con tale soggetto preveda espressamente tali obblighi di assistenza.

In caso di violazione della sicurezza che comporti 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, il soggetto nominato Responsabile del trattamento ha il compito di notificare la violazione, senza ingiustificato ritardo dal momento in cui ne è venuto a conoscenza, al Servizio dell'ERSA con cui mantiene i contatti diretti nell'ambito dei servizi svolti.

Il Responsabile del trattamento non deve valutare la probabilità di rischio sui diritti e le libertà delle persone fisiche derivante dalla violazione, in quanto tale compito spetta unicamente al Titolare del trattamento.

Il Direttore del Servizio dell'ERSA, non appena ricevuta comunicazione del *data breach*, deve mettersi in contatto con il Titolare del trattamento e fornire tutte le informazioni del caso.

Il Titolare del trattamento, con la cooperazione del dirigente della struttura con cui il Responsabile del trattamento mantiene i contatti diretti e del Responsabile della protezione dei dati, conclude una breve istruttoria per decidere se inviare la notifica al Garante.

Se al termine di tale istruttoria non si rileva la necessità di notifica, la procedura si conclude e si procede unicamente ad aggiornare il Registro dei data breach.

Se al contrario si riscontra la necessità della notifica al Garante, il Titolare procede in tal senso tramite PEC **entro 72 ore dall'avvenuta comunicazione dell'evento da parte del soggetto Responsabile del trattamento,** fornendo le seguenti informazioni:
- natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché categorie e numero approssimativo di registrazioni dei dati personali coinvolte dall'evento;

- nome e dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- probabili conseguenze della violazione dei dati personali;
- misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Titolare, coadiuvato dal RPD e dal dirigente del Servizio con cui il Responsabile del trattamento mantiene i contatti diretti nonché dal Responsabile stesso, effettua successivamente una breve istruttoria per valutare se notificare la comunicazione anche agli interessati, ai sensi dell'articolo 34 del GDPR.

Qualora il Titolare concluda l'istruttoria di cui sopra riconoscendo la sussistenza dei presupposti per la comunicazione agli interessati, dovrà attivarsi, in modo da fornire almeno le seguenti informazioni:
- descrizione della natura della violazione;
- nome e dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

In linea di principio, la violazione è comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura analoga che consenta di informare gli interessati con analoga efficacia.

Se viceversa l'istruttoria si conclude definendo la non necessità di comunicare la violazione all'interessato, il Garante può richiedere che tale comunicazione venga comunque effettuata, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato.

Il Titolare del trattamento, con la cooperazione del Responsabile della protezione dei dati e del dirigente del Servizio con cui il Responsabile del trattamento mantiene i contatti diretti nonché con il Responsabile stesso, provvede ad applicare tutte le misure necessarie per arginare i possibili danni conseguenti alla violazione, nonché ad adottare eventuali misure future necessarie per evitare il ripetersi dell'evento dannoso.

Tutte le azioni intraprese sono adeguatamente documentate e viene altresì aggiornato il Registro delle violazioni.