COMUNE DI MALO
PROVINCIA DI VICENZA

DETERMINAZIONE N. 745
Data di registrazione 29/10/2018

Oggetto: REGOLAMENTO UE 679/2016 (GDPR). APPROVAZIONE PROTOCOLLO DATA BREACH (PROTOCOLLO IN CASO DI VIOLAZIONE DEI DATI PERSONALI).

VICE SEGRETARIO
IL RESPONSABILE DEL SERVIZIO

Visto il D.L.gs n. 118 del 23.06.2011 e successive integrazioni e modificazioni riguardante le disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42;

Richiamata la deliberazione n. 85 in data 27.12.2017, dichiarata immediatamente eseguibile, con la quale il Consiglio Comunale ha approvato il Bilancio di previsione 2018-2020 ed i relativi allegati;

Richiamata la deliberazione di Giunta comunale n. 1 del 09.01.2018, dichiarata immediatamente eseguibile, con cui è stato approvato il PEG (Piano esecutivo di gestione) per gli anni 2018-2020;

Visto il decreto sindacale n. 1 in data 08.01.2018 con il quale è stato conferito al sottoscritto l'incarico di posizione organizzativa per l'anno 2018;

Premesso che:

- il Parlamento Europeo in seduta plenaria, il 14 aprile 2016, ha approvato il Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, anche noto come GDPR (General Data Protection Regulation), "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" che costituisce, con la Direttiva (UE) 2016/680 del 27 aprile 2016 dello stesso Parlamento europeo e del Consiglio, il c.d. "pacchetto protezione dati personali";
- Il nuovo Regolamento è stato pubblicato sulla Gazzetta Ufficiale Europea del 14 maggio 2016, è vigente dal 24 maggio 2016 ed applicabile a decorrere dal 25 maggio 2018 in tutti gli Stati membri; tale applicabilità ha il fine di trattare in modo omogeneo il tema della privacy sia nelle aziende private che presso le amministrazioni pubbliche dei diversi Paesi che compongono l'Unione;
- Il predetto Regolamento prevede che tutte le Pubbliche Amministrazioni (ad eccezione delle autorità giudiziarie) dovranno obbligatoriamente adeguarsi entro la data di applicazione e cioè entro il 25 maggio p.v.;

Dato atto che la nuova normativa europea attua un profondo mutamento culturale e, perciò, quanto richiesto agli Stati membri non può limitarsi alla osservanza di un mero adempimento formale in materia di privacy, ma deve porsi nella prospettiva di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie;

Considerate le principali novità introdotte dal RGPD, che riguardano in particolare:

- il recepimento del "principio di accountability" (obbligo di rendicontazione) che impone alle Pubbliche Amministrazioni, titolari del trattamento dei dati, di dimostrare di avere adottato le misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio, stabilendo che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento;
- L'introduzione della responsabilità diretta dei titolari del trattamento in merito al compito di assicurare ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali;
- La definizione della nuova categoria di dati personali (i c.d. dati sensibili di cui al precedente Codice Privacy);
- L'istituzione della figura obbligatoria del Responsabile della protezione dei dati -"Data Protection Officer"(DPO), incaricato di assicurare una gestione corretta dei dati personali negli enti;
- L'introduzione del Registro delle attività del trattamento in forma scritta o anche in formato elettronico, ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate e che dovrà contenere specifici dati indicati dal RGPD;
- L'obbligo, a carico dell'ente, di effettuare la valutazione di impatto sulla protezione dei dati, prima di procedere al trattamento, soprattutto quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- La reintroduzione dell'obbligatorietà della redazione del documento programmatico sulla sicurezza (DPS), obbligo previsto dal D.Lgs. 196/2003 e abrogato dal Decreto Legge n. 5 del 9 febbraio 2012, convertito dalla legge n. 35 del 4 aprile 2012;
- Il rafforzamento dei poteri delle Autorità Garanti nazionali e l'inasprimento delle sanzioni amministrative a carico di imprese e pubbliche amministrazioni in caso di violazioni dei principi e disposizioni del Regolamento;

Preso atto che per quanto riguarda la sicurezza del trattamento dei dati il Regolamento UE 679/2016 stabilisce una serie di principi in materia di sicurezza del trattamento dei dati personali, imponendo al titolare del trattamento ed ai responsabili del trattamento di adottare tutte le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il titolare o i responsabili dovrebbero valutare i rischi inerenti al trattamento ed adottare le misure per limitare tali rischi, quali la cifratura. Tali misure devono assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare un danno fisico, materiale o immateriale.

Evidenziato quindi che l'elemento chiave di qualsiasi policy sulla sicurezza dei dati deve essere quello di evitare la loro violazione e, qualora questo dovesse accadere, di reagire in modo tempestivo;

Visto il "Protocollo Data breach" (protocollo in caso di violazione dei dati personali), predisposto dal DPO incaricato e allegato alla presente, il quale si propone di fornire una serie di informazioni sul concetto di violazione dei dati personali nonché di individuare le procedure da seguire in caso di avvenuta violazione, nel rispetto di quanto disposto dal GDPR;

Ritenuto di approvare il suddetto documento;

Verificato, ai sensi dell'art. 9, comma 1, lett. a), numero 2 del D.L. 78/2009, convertito con L. 102/2009, il preventivo accertamento della compatibilità del programma dei pagamenti conseguente al presente atto con le regole di finanza pubblica e la programmazione dei flussi di cassa;

Visto il D.Lgs 50/2016;

Visto il D.Lgs. n. 267 del 18.08.2000;

Visto lo Statuto Comunale ed il Regolamento per l'ordinamento degli uffici e dei servizi;

DETERMINA

1. di approvare "Protocollo Data breach" (protocollo in caso di violazione dei dati personali), predisposto dal DPO incaricato e allegato alla presente;

2. di precisare che il suddetto documento si propone di fornire una serie di informazioni sul concetto di violazione dei dati personali nonché di individuare le procedure da seguire in caso di avvenuta violazione, nel rispetto di quanto disposto dal GDPR;

3. di trasmettere copia del "Protocollo Data breach" a tutti i dipendenti.

*****

Si esprime parere favorevole di regolarità tecnica ai sensi dell'art. 147 bis del D.Lgs n. 267/2000.

Malo, 29/10/2018

IL RESPONSABILE DEL SERVIZIO
Oscar Raumer

(Documento firmato digitalmente)

DATA BREACH

Protocollo in caso di violazione dei dati personali ai sensi degli articoli 33 e seguenti Regolamento UE 679/2016 (Regolamento generale sulla protezione dei dati)

INDICE

1. Premessa

La sicurezza del trattamento dei dati (art. 32 e considerando 83 Regolamento UE 679/2016)

Il Regolamento UE 679/2016 ("Regolamento generale sulla protezione dei dati", di seguito "GDPR") stabilisce una serie di principi in materia di sicurezza del trattamento dei dati personali, imponendo al titolare del trattamento ed al responsabile del trattamento di adottare tutte le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il titolare o il responsabile dovrebbe valutare i rischi inerenti al trattamento ed adottare le misure per limitare tali rischi, quali la cifratura. Tali misure devono assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare un danno fisico, materiale o immateriale.

L'elemento chiave di qualsiasi policy sulla sicurezza dei dati deve essere quindi quello di evitare la loro violazione, e, qualora questo dovesse accadere, di reagire in modo tempestivo.

Il presente documento si propone di fornire una serie di informazioni sul concetto di violazione dei dati personali nonché di individuare le procedure da seguire in caso di avvenuta violazione, nel rispetto di quanto disposto dal GDPR.

2. Definizioni generali

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

Titolare del trattamento: 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.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

3. Definizione di data breach

La violazione dei dati personali, o "*data breach*", è definita all'art. 4 del GDPR come la "**violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".**

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione ai loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudominizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata (vd. considerando 85 GDPR).

Le linee guida del WP29 ("Article 29 Data Protection Working Party") del 03.10.2017 "*Guidelines on Personal data breach notification under Regulation 2016/679*" specificano che le violazioni possono essere suddivise nelle seguenti categorie:

1) violazioni di riservatezza: nel caso in cui si verifichi una divulgazione o un accesso a dati personali non autorizzato od accidentale;

2) violazioni di integrità: nel caso in cui si verifichi una modifica dei dati non autorizzata od accidentale;

3) violazioni di disponibilità: nel caso in cui si verifichi una non autorizzata od accidentale perdita delle credenziali di accesso o una distruzione dei dati.

La violazione dei dati, a seconda delle circostanze, può rientrare in uno solo dei casi di cui sopra, o in tutti e tre.

La violazione dei dati non deve essere celata, in quanto l'oscuramento della notizia, oltre a esporre il titolare del trattamento a gravi sanzioni amministrative pecuniarie, amplifica in modo sensibile gli effetti negativi dell'evento e può ostacolare la tutela dell'interessato.

4. Adempimenti da svolgere in caso di data breach

Qualora si verifichi un evento che possa comportare la violazione di dati personali, è necessario contattare **immediatamente** i seguenti soggetti:

- Paola Lain, sindaco di Malo, e-mail ----- PEC malo.vi@cert.ip-veneto.net telefono 0445.585211
- avv. Anna Perut, DPO del Comune di Malo, e-mail dpo@regolateam.it, PEC anna.perut@avvocatipordenone.it, telefono 0434.360253, cellulare 333.3511390
- PASUBIO TECNOLOGIA s.r.l., via Ventinove Aprile n. 6, 36015 Schio (VI), telefono 0445.610511, e-mail info@altovicentino.net

L'obbligo di informazione grava anche sui responsabili del trattamento, i quali devono informare il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione. La comunicazione deve essere tempestiva, in modo da permettere al titolare di rispettare i termini per gli adempimenti di cui all'art. 33 GDPR. Il responsabile deve comunicare al titolare qualsiasi violazione dei dati personali, a prescindere dai possibili rischi derivanti dalla violazione.

Una volta ricevuta la notizia di un potenziale *data breach*, il titolare, coadiuvato da esperti qualificati in campo informatico e legale, dovrà procedere immediatamente con le indagini più opportune volte ad accertare se effettivamente si sia verificata una violazione, raccogliendo tutte le prove e indizi possibili. Nel contempo, a seconda del tipo di violazione, dovrà adottare tutte le

misure per limitare la violazione e recuperare gli eventuali dati persi, implementare il livello di sicurezza dei dati, istruendo in modo adeguato tutti i dipendenti.

4.1 Notifica al Garante

In base all'art. 33 GDPR, **il titolare del trattamento deve notificare al Garante la violazione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza dell'evento, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.**

Decorso il termine di 72 ore, la notifica della violazione deve essere corredata dalle ragioni del ritardo.

Il termine di 72 decorre dal momento in cui il titolare ha avuto conoscenza della violazione dei dati, ovvero quando il titolare ha avuto un **ragionevole livello di certezza** circa l'avvenimento di un incidente alla sicurezza che ha determinato la compromissione di dati personali.

La consapevolezza della violazione dei dati personali può dipendere molto dalle circostanze, perché alcune violazioni possono essere facilmente individuabili, altre invece possono richiedere un'indagine più approfondita. Durante le indagini, il titolare può essere considerato come privo di un grado di conoscenza tale da far scattare immediatamente l'obbligo di notifica. Ciò precisato, il WP29 sottolinea che il diligente comportamento del titolare sarà in ogni caso valutato sulla base della sua tempestiva attivazione in caso venga informato di una possibile infrazione. La fase investigativa, quindi, non deve essere abusata per prorogare illegittimamente il termine di notifica.

Di seguito si riportano alcuni esempi chiarificatori elaborati dal WP29:

1. perdita di una chiavetta USB i cui dati non sono cifrati: benché non sia possibile avere la certezza se un soggetto non autorizzato acceda o meno ai dati, la perdita della chiavetta rientra senza dubbio nei casi di violazione alla disponibilità dei dati, e la consapevolezza della violazione si ha nel momento in cui il titolare scopre lo smarrimento della chiavetta.

2. un soggetto terzo comunica al titolare di aver accidentalmente ricevuto dati relativi ad un suo cliente, mostrandogli prove adeguate. Il titolare diventa consapevole della violazione nel momento in cui riceve prove della stessa.

3. Il titolare scopre che c'è stata una possibile intrusione nel suo sistema, e nell'eseguire i controlli necessari, scopre che i dati ivi contenuti siano stati compromessi, momento nel quale il titolare diventa consapevole della violazione.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione. In base a quanto precisato dal WP29, è opportuno distinguere in modo adeguato le categorie di interessati, ad esempio: dipendenti, clienti, persone con disabilità, minori e altre categorie vulnerabili, nonché i tipi di dati: dati relativi alla salute, informazioni sulla sicurezza sociale, informazioni finanziarie, coordinate bancarie, dettagli dei documenti di riconoscimento). Qualora la violazione comporti dei seri rischi per l'interessato (es. furto di identità, perdite finanziarie), la notifica deve fare chiaro riferimento a queste categorie di dati. Qualora non sia possibile avere informazioni precise sul numero di

interessati e di dati oggetto di violazione, la notifica deve essere comunque fatta nei termini, indicando le predette informazioni in numero approssimativo, specificando in seguito il numero esatto.

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati (ove esistente) o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere 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.

La notifica può essere effettuata utilizzando il modello allegato alla presente policy (all. 1).

4.1.1 Notifica in fasi

L'art. 33, paragrafo 4, GDPR, prevede la possibilità di procedere alla "notifica in fasi", stabilendo che "*qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*". L'ipotesi riguarda prevalentemente i casi di violazioni molto complesse, nelle quali è necessario svolgere indagini approfondite per comprendere la natura della violazione e la misura in cui la violazione ha coinvolto i dati.

Alla luce di questo, qualora per la complessità o estensione della violazione, il titolare non sia in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie, potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di *alert*, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri. Al momento della notifica, il titolare deve comunicare al Garante che provvederà a trasmettere in un secondo momento tutti i dettagli relativi alla violazione.

Il WP29 ha precisato che non incorre in alcuna sanzione il titolare che, dopo la notifica iniziale, abbia scoperto che l'incidente alla sicurezza sia stato arginato e non vi sia stata un'effettiva violazione dei dati personali. In questi casi, il titolare potrà aggiornare il Garante in tal senso, comunicandogli che in realtà non vi è stata una violazione di dati.

4.1.2 Casi in cui non è obbligatoria la notifica al Garante.

L'art. 33, paragrafo 1, GDPR, precisa che **la notifica non è necessaria se è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.**

Il WP29 ha precisato che tale ipotesi ricorre in caso di violazione di dati già disponibili al pubblico, o nel caso in cui i dati siano crittografati e la chiave di decifratura non sia stata compromessa. In quest'ultimo caso, qualora in seguito il titolare scopra che la chiave in realtà è stata violata, allora dovrà procedere obbligatoriamente alla notifica.

Il titolare, quindi, è tenuto a effettuare un'attenta analisi sugli effetti che la violazione può comportare sui diritti degli interessati, al fine di decidere se procedere o meno alla notifica al Garante.

4.1.3 Sanzioni in caso di omessa notifica

La violazione degli obblighi del titolare del trattamento o del responsabile del trattamento previsti dagli articoli 33 e 34 GDPR comporta sanzioni pecuniarie fino a 10.000.000,00 €, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4.2 Comunicazione della violazione dei dati personali all'interessato (art. 34 GDPR)

In base all'art. 34 GDPR, **il titolare del trattamento è tenuto a comunicare la violazione all'interessato, senza ingiustificato ritardo, nei casi in cui la violazione dei dati personali è probabile che presenti un rischio elevato per i diritti e le libertà delle persone fisiche.**

La comunicazione all'interessato di cui al paragrafo 1 dell'art. 34 GDPR 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'articolo 33, paragrafo 3, lettere b), c) e d), GDPR, ovvero:

- la descrizione della natura della violazione;

- il nome e i contatti del responsabile della protezione dei dati personali (ove esistente) o di altro punto di contatto;

- una descrizione delle possibili conseguenze della violazione;

- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati e anche, se del caso, per attenuarne i possibili effetti negativi. E' opportuno che il titolare suggerisca agli interessati i possibili accorgimenti per proteggersi dagli effetti della violazione, come modificare le password.

La comunicazione deve essere effettuata privilegiando modalità di comunicazione dirette con gli interessati, ad esempio e-mail, SMS, messaggi diretti, utilizzando il modello allegato alla presente policy (all. 2). E' opportuno evitare di inviare la comunicazione nel contesto di newsletter o update generali, in quanto gli interessati potrebbero non cogliere l'importanza del messaggio e confonderla con le comunicazioni periodiche. E' necessario tenere in considerazione la nazionalità degli interessati, in modo da inviare la comunicazione nella loro lingua.

Il considerando 88 precisa altresì che nel definire le modalità e le procedure applicabili alla notifica delle violazioni di dati personali, sia opportuno tenere in considerazione anche i legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali. Di conseguenza, se richiesto dalle autorità investigative, la comunicazione agli interessati può essere rinviate per il tempo necessario per lo svolgimento delle opportune attività di indagine.

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 dell'art. 34 GDPR se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) 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 di cui al paragrafo 1, art. 34 GDPR. Es. qualora il titolare del trattamento abbia individuato immediatamente il responsabile della violazione ed impedito che lo stesso potesse compiere qualsiasi azione in relazione ai dati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Es. allagamento di un archivio di documenti pubblici, conservati in forma solo cartacea. In questo caso la comunicazione agli interessati può essere fatta mediante comunicazione pubblica.

Da ultimo, si ricorda che nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3, articolo 34 GDPR, sia soddisfatta.

5. Valutazione dei rischi

E' opportuno sottolineare la differenza dei presupposti che impongono la notifica della violazione al garante e la comunicazione agli interessati, in quanto:

- la notifica al Garante è obbligatoria a meno che sia improbabile che la violazione presenti **rischi** per i diritti e le libertà delle persone fisiche;
- la comunicazione della violazione agli interessati è obbligatoria quando è probabile che presenti **un rischio elevato** per i diritti e le libertà delle persone fisiche.

Per valutare i rischi connessi alla violazione, il titolare deve prendere in considerazione i seguenti aspetti:

- il tipo di violazione: il tipo di violazione può influire sul livello di rischi cagionati agli interessati. Es. la divulgazione di dati sanitari a soggetti non autorizzati può comportare effetti diversi rispetto alla distruzione del dato sanitario.
- la natura del dato: la violazione di dati particolari (sensibili) è più dannosa rispetto alla violazione di dati non particolari, così come la violazione di dati particolarmente delicati (es. dati relativi ai documenti di identità, dati finanziari, numeri di carta di credito)
- grado di identificazione degli interessati: un ulteriore aspetto da valutare è il livello di facilità con il quale è possibile a risalire alle generalità dei singoli interessati soggetti alla violazione. Es. il furto di dati identificativi o di dati facilmente individuabili presenta livelli di rischio più elevati di dati crittografati.

- gravità delle conseguenze sugli interessati: la gravità può dipendere non solo dal tipo di dato violato ma anche dalle intenzioni e dall'utilizzo che gli autori della violazione intendono fare.
- caratteristiche degli interessati: la violazione di dati relativi a minori o altre categorie delicate può presentare rischi più elevati.
- tipo di attività svolta dal titolare: il tipo di attività svolta dal titolare può influire sul livello di rischio per gli interessati (es. attività sanitaria).
- numero di soggetti coinvolti: in genere, la violazione di dati relativi a numeri elevati di individui comporta rischi più elevati.

6. Registro delle violazioni (art. 33, paragrafo 5, GDPR)

A prescindere dall'obbligo di notifica al Garante e di comunicazione agli interessati, il titolare deve tenere il registro delle violazioni nel quale documentare qualsiasi violazione, sulla base del modello allegato al presente protocollo (all. 3). Il registro deve indicare:

- le circostanze relative alla violazione;
- le conseguenze;
- i provvedimenti adottati per porvi rimedio.

Nel registro devono essere annotate tutte le decisioni adottate dal titolare in occasione del data breach, quale ad esempio la decisione di non effettuare la notifica al Garante, o in caso di notifica tardiva, i motivi del ritardo.

7. Esempi

Il WP29 ha predisposto una serie di esempi volti ad illustrare corretti modelli di comportamento a fronte di possibili dati personali.

a) Un titolare del trattamento ha archiviato la copia di backup di un archivio di dati personali su una chiavetta USB, proteggendoli con un algoritmo crittografico. La chiavetta viene rubata durante una effrazione.

Notifica al Garante? NO

Notifica all'interessato? NO

N.B. se in seguito emerge che la chiave è stata violata, è necessario procedere con la notifica al Garante.

b) Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico, i dati personali degl'interessati vengono catturati. Il titolare ha a che fare solo con interessati che si trovano in Paesi dell'Unione Europea.

Notifica al Garante? SI

Notifica all'interessato? SI

c) Una breve interruzione dell'alimentazione elettrica che si è protratta per alcuni minuti nella segreteria del titolare impedisce ai clienti di chiamare l'ente per accedere ai propri dati.

Notifica al Garante? NO

Notifica all'interessato? NO

N.B. tale evento è comunque da segnalare nel registro delle violazioni.

d) Un interessato telefona al call center di una banca, riferendo di aver ricevuto un estratto conto di un altro cliente. Dopo una rapida indagine di 24 ore, il titolare accerta con una ragionevole certezza l'avvenuta violazione del sistema.

Notifica al Garante? SI

Notifica all'interessato? SI

e) Un titolare gestisce un sito di vendite on line ed opera con clienti di numerosi Stati membri. Il sito online è vittima di un attacco informatico e vengono pubblicate on line dall'hacker le credenziali di accesso e lo storico degli acquisti del clienti.

Notifica al Garante? SI

Notifica all'interessato? SI

f) Un'email di marketing diretto viene inviata ai destinatari indicandoli nei campi "a" e "cc", con la conseguenza che tutti i destinatari possono leggere gli indirizzi e-mail degli altri destinatari.

Notifica al Garante? SI, qualora siano stati coinvolti un vasto numero di soggetti, si tratti di dati particolari di salute (es. mailing list di uno psicoterapeuta) o vi siano altri elementi di rischio.

Notifica all'interessato? SI, a seconda del tipo di dato coinvolto e della gravità delle possibili conseguenze.

Allegato 1

Modello notifica al Garante ai sensi dell'art. 33 del Regolamento UE 679/2016

Spettabile Garante,

Io scrivente Comune di Malo, in qualità di titolare del trattamento, con la presente comunica l'avvenuta violazione di dati personali, di seguito meglio specificata.

La natura della violazione è la seguente
descrivere la violazione in modo completo, includendo le date e le ore in cui si è verificata la violazione

Questa violazione riguarda i dati personali di
indicare il numero degli interessati e la descrizione della categoria degli interessati i cui dati sono stati violati, specificando anche l'eventuale coinvolgimento di dati particolari

Le probabili conseguenze della violazione dei dati sono le seguenti
indicare le probabili conseguenze della violazioni

Misure adottate e proposte al fine di attenuare i possibili effetti negativi
Per porre rimedio alla violazione e per attenuare i possibili effetti negativi abbiamo adottato le seguenti misure: elencare il piano per affrontare e risolvere la violazione, comprese le riunioni degli esperti chiamati a risolvere il problema, le indagini avviate, le azioni correttive e le future modifiche al flusso di dati che ha subito la violazione.

Ulteriori informazioni su questa violazione possono essere richieste al DPO avv. Anna Perut (e-mail dpo@regolateam.it - PEC anna.perut@avvocatipordenone.it, telefono 0434.360253, cellulare 333.3511390).

Cordiali saluti.

Il Comune di Malo

Allegato 2

Modello comunicazione di una violazione di dati personali agli interessati ai sensi dell'art. 34 del Regolamento UE 679/2016

Gentile Signora, Egregio Signore,

con la presente Le comunichiamo che purtroppo si è verificata una violazione dei nostri sistemi informatici che ha riguardato anche i Suoi dati personali.

La violazione è stata prontamente affrontata dai nostri esperti di sicurezza informatica ed esperti legali per ridurre ulteriormente l'esposizione dei Suoi dati personali e le possibili conseguenze della violazione. Ci stiamo adoperando per fare tutto quanto è in nostro potere per garantire che il danno sia mitigato e che ciò non accada di nuovo in futuro.

In ottemperanza a quanto disposto dall'art. 34 del Regolamento UE 679/2016, è obbligo dello scrivente Comune fornirLe in modo chiaro e semplice tutte le informazioni relative alla violazione, in modo da arginare il più possibile le conseguenze della violazione stessa.

Cosa è accaduto
descrivere la violazione, precisando la cronologia degli eventi, senza indicare informazioni sensibili sul Comune, a meno che non sia indispensabile per descrivere la violazione

Dati personali coinvolti
Elencare i tipi di dati personali.

Conseguenze della violazione
Descrivere le probabili conseguenze della violazione, tenuto conto della natura della violazione e dei tipi di dati personali coinvolti.

Misure adottate e proposte al fine di attenuare i possibili effetti negativi
Per porre rimedio alla violazione e per attenuare i possibili effetti negativi abbiamo adottato le seguenti misure:

Le suggeriamo di …… (elencare le azioni che l'interessato dovrà approntare)

Come eviteremo in futuro tale problematica
Al fine di evitare che tale violazione si verifichi nuovamente e di ridurre al minimo l'impatto sui cittadini abbiamo attivato le seguenti azioni:
elencare le azioni intraprese dal Comune per garantire che questa violazione non venga ripetuta, senza compromettere la riservatezza dell'organizzazione, rassicurando nel contempo l'interessato.

E' stata effettuata la notifica al Garante ai sensi dell'art. 33 Regolamento UE 679/2016.

Per ulteriori informazioni si prega di contattare il DPO avv. Anna Perut (e-mail dpo@regolateam.it - PEC anna.perut@avvocatipordenone.it, telefono 0434.360253).

Cordiali saluti

Allegato 3

Registro delle violazioni

N°	Dettagli violazione						Conseguenze della violazione	Misure correttive intraprese			
	Data	N° interessati	Origine violazione	Descrizione della violazione	Come siamo venuti a conoscenza della violazione	Descrizione della perdita di dati		Comunicazione agli interessati	Azioni correttive intraprese	Notificazione al Garante	Data di chiusura della violazione

COMUNE DI MALO
PROVINCIA DI VICENZA

DETERMINAZIONE N. 745
Data di registrazione 29/10/2018

Oggetto: REGOLAMENTO UE 679/2016 (GDPR). APPROVAZIONE PROTOCOLLO DATA BREACH (PROTOCOLLO IN CASO DI VIOLAZIONE DEI DATI PERSONALI).

PARERE DI REGOLARITA' CONTABILE E VISTO ATTESTANTE LA COPERTURA FINANZIARIA AI SENSI DELL'ARTICOLO 147 BIS DEL TUEL.
VISTO DI REGOLARITA' CONTABILE (art.183 comma 7 TUEL)

SI ATTESTA la regolarità contabile e la copertura finanziaria della determinazione di cui all'oggetto.

Annotazioni:

IMPEGNI

Capitolo	Anno	Descrizione Imp.	Importo	Imp.	Anno

ACCERTAMENTI

Capitolo	Anno	Descrizione Acc.	Importo	Acc.	Anno

Malo, 29/10/2018

SERVIZIO FINANZIARIO
IL RESPONSABILE DEL SERVIZIO
dott.ssa Claudia Boschetti

(Documento firmato digitalmente)

Questo documento è collegato digitalmente alla determina con timbro HASH (SHA1):
c03dd06a937f45b20f0d5de5b226c7592e662afe