COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 188 del 12/07/2019

OGGETTO: ARTICOLI 33 E 34 DEL REGOLAMENTO (UE) 2016/679. ADOZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI ("DATA BREACH")

L'anno **duemiladiciannove** il giorno **dodici** del mese di **luglio** alle ore **11:00** in Cittadella, nella sala delle adunanze la Giunta Comunale si è riunita con la presenza dei Signori:

PIEROBON LUCA	SINDACO	Presente
SIMIONI MARCO	ASSESSORE	Presente
BELTRAME MARINA	ASSESSORE	Presente
GALLI DIEGO	ASSESSORE	Presente
PAVAN FRANCESCA	ASSESSORE	Presente
DE ROSSI FILIPPO	ASSESSORE	Assente

Presenti n. 5 **Assenti n. 1**

Partecipa alla seduta il VICE SEGRETARIO SARTORE CARLO che provvede alla redazione del presente verbale.

Assume la presidenza il Sig. PIEROBON LUCA, nella sua qualità di SINDACO, il quale riconosciuta legale l'adunanza, dichiara aperta la seduta ed invita i presenti a deliberare sull'oggetto sopra indicato.

Deliberazione n. 188 del 12/07/2019

Viene esaminata la seguente proposta di delibera redatta dal Responsabile del Servizio, sulla quale sono stati espressi i pareri ai sensi dell'art. 49, comma 1 del D. Lgs. 267/2000.

OGGETTO: ARTICOLI 33 E 34 DEL REGOLAMENTO (UE) 2016/679. ADOZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI ("DATA BREACH")

LA GIUNTA COMUNALE

PREMESSO che in data 25.05.2018 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio di data 27.04.2016, 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) e rilevato inoltre che in data 19.09.2018 è entrato in vigore il D.lg. 10.08.2018 n. 101 di armonizzazione al Regolamento (UE) 2016/679;

EVIDENZIATO come il Regolamento (UE) 2016/679 – denominato “Regolamento generale sulla protezione dei dati”, in sigla RGPD – detti una nuova disciplina in materia di trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il “principio di responsabilizzazione” (c.d. accountability) e ponendo al centro del nuovo quadro normativo la figura del “Responsabile della protezione dei dati”, in sigla RPD;

SOTTOLINEATO come il Comune di Cittadella sia tenuto, a seguito dell’entrata in vigore del Regolamento (UE) 2016/679, ad una serie di adempimenti conseguenti;

RICHIAMATA la delibera di Giunta Municipale n. 105 del 23 maggio 2018, con la quale il Comune di Cittadella ha designato il Responsabile della protezione dei dati la Ditta Boxxapps Srl, via Torino 180, Mestre - Venezia (P. IVA 04155080270);

ACCERTATO come tra gli adempimenti obbligatori rientri quello previsto dagli artt. 33 e 34 del Regolamento (UE) 2016/679, e segnatamente quello relativo all’adozione di una specifica procedura disciplinante la gestione delle violazioni dei dati personali (“data breach”);

ESAMINATA la proposta di cui trattasi e ritenuta la stessa meritevole di approvazione in quanto rispondente alle finalità ed ai contenuti previsti dagli artt. 33 e 34 del Regolamento (UE) 2016/679;

ACQUISITO il parere favorevole in ordine alla sola regolarità tecnica da parte del responsabile del servizio competente per materia;

DATO ATTO che non necessita acquisire il parere di regolarità contabile in quanto la presente proposta di deliberazione non comporta aspetti di natura finanziaria;

VISTO il Regolamento (UE) 2016/679, e in particolare gli artt. 33 e 34. Visto il D.lg. 10.08.2018 n. 101;

VISTO il D. Lgs. 267/2000 recante il Testo Unico sull'Ordinamento degli Enti Locali";

DELIBERA

1. di adottare, per tutto quanto indicato in premessa e qui inteso come integralmente riportato, la procedura disciplinante la gestione delle violazioni dei dati personali ("data breach") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, allegata alla presente deliberazione per formarne parte integrante e sostanziale;
2. di attestare la pubblicazione di cui all'art. 23 del D.Lgs. 33/2013;
3. di dare atto dell'avvenuto assolvimento degli obblighi di astensione di cui agli artt. 5 e 6 del codice di comportamento approvato con deliberazione di Giunta Comunale n. 12/2014 e dell'art. 6-bis della L. 241/90 e, pertanto, in ordine al presente provvedimento non sussiste situazione di conflitto di interessi né in capo al responsabile del procedimento, né in capo ai soggetti che sottoscrivono a vario titolo il presente atto, né in capo a chi partecipa, a qualsiasi titolo a detto procedimento;
4. di dichiarare con votazione autonoma e separata, per motivi urgenti connessi alla necessità di attuare tempestivamente la normativa in materia di privacy, la presente deliberazione immediatamente eseguibile ai sensi e per gli effetti dell'art. 134 del Decreto Legislativo n. 267/2000.

LA GIUNTA COMUNALE

Vista la su estesa proposta di delibera;

Avuti i prescritti pareri favorevoli a termini ai sensi dell'art. 49, 1° comma del decreto legislativo 18.08.2000 n. 267, “Testo Unico delle leggi sull'ordinamento degli Enti Locali” espressi sulla proposta di delibera e riportati a conferma in calce alla presente;

Con voti unanimi e favorevoli, palesemente espressi

DELIBERA

1 di approvare e far propria la proposta di delibera sopra riportata nella sua formulazione integrale, ovvero senza alcuna modificazione o integrazione;

2 di comunicare la presente delibera ai capigruppo consiliari ai sensi dell'art. 125 del D. Lgs. 267/2000;

*****

Con apposita votazione, favorevole ed unanime, il presente atto è dichiarato immediatamente eseguibile ai sensi dell'art. 134 comma 4 del D.Lgs 267/2000.

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

Verbale n. **32** del **12**.**07**.**2019**

IL SINDACO
PIEROBON LUCA

IL VICE SEGRETARIO
SARTORE CARLO

COMUNE DI CITTADELLA

PROVINCIA DI PADOVA

Istruzione per la gestione del Data Breach

Revisione	Data di emissione	Motivo della revisione	Visto preparazione	Visto approvazione	Estremi di approvazione
00	01/07/2019	Prima emissione	Emanuele Nichele	Giunta Municipale	

SOMMARIO

1 SCOPO E CAMPO DI APPLICAZIONE

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, quali ad esempio la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno[1] economico o sociale significativo per la persona fisica interessata[2]. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento ha l'obbligo di notificarla, ai sensi dell'art. 33 Regolamento (UE) 2016/679, all'Autorità di Controllo competente, 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. Qualora la notifica all'Autorità di Controllo, e dunque al Garante per la Protezione dei Dati Personali,

[1] Si veda la guida dell'Information Commissioner's Office, anche detta ICO, pubblicata al link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection regulation-gdpr/personal-data-breaches/, che afferma come "*un data breach può avere un range di diversi effetti sugli individui, che includono ad esempio uno stress emotivo, ma anche danni fisici e materiali. Alcuni data breach possono non comportare rischi particolari per gli interessati. Altre violazioni invece possono colpire in modo significativo gli interessati coinvolti. Per tali ragioni il titolare del trattamento deve valutare le violazioni caso per caso, soffermandosi su elementi specifici*".

[2] Si veda il considerando numero 85 del Regolamento (UE) 2016/679.

non sia effettuata entro 72 ore, la comunicazione deve essere corredata dei motivi del ritardo[3].

L'art. 34 Regolamento (UE) 2016/679 prevede poi che:

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 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;

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.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo 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 è soddisfatta".

La comunicazione, dunque, deve descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata, tese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'Autorità di Controllo, nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge[4].

Al fine di ottemperare al meglio agli obblighi imposti dagli artt. 33 e 34 Regolamento (UE) 2016/679, è opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se ci sia stata violazione dei dati personali e dunque informare tempestivamente l'autorità di controllo e l'interessato. È opportuno, inoltre, provvedere alla trasmissione della notifica senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze ed effetti negativi per l'interessato. Siffatta notifica, infatti, potrebbe

[3] Il considerando numero 85 del Regolamento (UE) 2016/679 prevede infatti che "*le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo*".

[4] Su tale punto, si veda il Considerando numero 86 del Regolamento (UE) 2016/679, che prevede "*Ad esempio, la necessità di attenuare un rischio immediato di danno, richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*".

dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal Regolamento (UE) 2016/679[5].

Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione, atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei 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[6].

Ritenuta l'abolizione degli obblighi generali e indiscriminati di notifica all'Autorità di Controllo, essi devono essere opportunamente sostituiti con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo ed in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale[7].

Nei casi in cui le misure di sicurezza non siano in grado di contrastare le minacce o risultino limitatamente efficaci nella prevenzione di eventi avversi alla sicurezza del dato (es. compromissione di un sistema, accesso non autorizzato alle informazioni), l'Ente deve avere la capacità di rispondere rapidamente ed efficacemente a un potenziale incidente, riducendo gli impatti e limitando la possibilità di occorrenze future.

2 IDENTIFICAZIONE DELLE RESPONSABILITÀ

L'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti è un elemento indispensabile per assicurare il corretto governo della procedura da attuare nel caso di violazione dei dati personali e permettere un'efficace operatività, intesa come attuazione di quanto in seguito esposto.
Si ritiene fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità in tale ambito, correlate allo svolgimento della attività lavorative. In particolare, ai vertici dell'organizzazione, che di fatto sono i responsabili ultimi nel caso di violazione dei dati personali all'interno dell'organizzazione.

Nel caso in cui si verifichi un data breach, il titolare del trattamento notifica la violazione all'Autorità di Controllo competente a norma dell'articolo 33 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.

La norma in questione prevede infatti che:

"*1. 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,*

[5] Si veda su tale punto il Considerando numero 87 del Regolamento (UE) 2016/679.

[6] Si veda sul punto il Considerando numero 88 del Regolamento (UE) 2016/679.

[7] Si veda sul punto il Considerando numero 89 del Regolamento (UE) 2016/679.

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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 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;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati 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.

4. 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.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

È la stessa norma ad individuare, quindi, i ruoli e le responsabilità dei soggetti privacy nella procedura per la gestione del data breach, ruoli che vengono schematizzati qui di seguito.

Titolare del trattamento (Process Owner)

- Notifica la violazione all'Autorità di Controllo competente a norma dell'articolo 33 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.
- Documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di Controllo di verificare il rispetto del presente articolo.
- Monitora ogni evento che riguardi la possibile violazione dei dati personali

Responsabile del trattamento

- Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
- Monitora ogni evento che riguardi la possibile violazione dei dati personali

Responsabile per la Protezione del Dato (DPO/RPD)

- Deve sempre essere informato di tutte le fasi inerenti la violazione, gli accertamenti e le notifiche obbligatorie

Privacy Manager

- Deve ricevere le segnalazioni di eventi che possono riguardare violazioni di dati personali, nonché coordinare le verifiche ed occuparsi di fungere da punto di contatto con il DPO e con l'Autorità di Controllo (una volta effettuata la notifica).

Amministratore di Sistema

- Coadiuva il titolare o il responsabile per documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Il titolare o il responsabile seguono le istruzioni impartite dall'Amministratore di sistema.

Delegati, autorizzati al trattamento ed interessati

- Coadiuvano il titolare o il responsabile per le attività richieste a contenimento delle violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
- Seguono le istruzioni impartite.
- Procedono a segnalare al Privacy Manager ogni evento che possa riguardare una violazione dei dati personali.

3 DEFINIZIONI

- **Dato Personale**: 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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile**.**
- **"Data Breach", Violazione Dei Dati Personali**: Ai sensi dell'art. 4 num. 12) Regolamento (UE) 2016/679, si definisce data breach, o violazione dei dati personali "*la 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*". La violazione dei dati personali, dunque, include violazioni che sono il risultato di cause sia accidentali che intenzionali; ciò significa anche che la violazione è qualcosa di più della mera perdita di dati[8]. Il presente modello organizzativo illustra la procedura di gestione da attuare

[8] Si veda la guida dell'Information Commissioner's Office, anche detta ICO, pubblicata al link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection regulation-gdpr/personal-data-breaches/, che prevede che esempi di data breach siano: "*accesso*

nel caso in cui si verifichi una violazione dei dati personali come sopra appena descritta.

4 MONITORAGGIO DELLE PROTEZIONI DEI DATI PERSONALI

Al fine di provvedere ad una corretta gestione della procedura per far fronte ad una violazione dei dati personali è necessaria la verifica costante delle condizioni di sicurezza per la protezione delle informazioni personali. Tale verifica deve essere effettuata sulle misure tecniche organizzative identificate per i vari trattamenti, al fine non solo di definire nel più breve tempo possibile la causa che ha portato alle violazioni dei dati personali ma anche allertarsi immediatamente di fronte ad una possibile violazione dei dati personali.

5 IDENTIFICAZIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Un data breach, dunque, si configura come un incidente di sicurezza che colpisce la riservatezza, l'integrità o la disponibilità del dato personale. In breve, si ravviserà un data breach ogni qual volta che un dato personale sia perso, distrutto, corrotto o rivelato: ad esempio nel caso in cui un soggetto, in assenza di autorizzazione, acceda o diffonda il dato, o nel caso in cui questo sia reso indisponibile, ad esempio quando sia stato "bloccato" da un ransomware, o accidentalmente perso o distrutto[9].

Per una corretta gestione delle violazioni dei dati personali è necessario aver provveduto ad una corretta mappatura dei dati contenenti informazioni personali, al fine di poter identificare, in ogni momento:

- Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.
- Le finalità del trattamento.
- L'identificazione delle categorie di interessati e delle categorie di dati personali.
- L'identificazione delle categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi.
- L'identificazione, se presenti, dei trasferimenti di dati personali verso paesi terzi e la loro identificazione.
- L'identificazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati.

effettuato da un soggetto terzo non autorizzato, azione (od omissione) deliberata o accidentale posta in essere da un titolare o da un responsabile del trattamento; l'inoltro di dati personali al mittente sbagliato; il furto o la perdita di dispositivi portatili contenenti dati personali; alterazioni o modifiche non autorizzate di dati personali; perdita di disponibilità dei dati personali".

[9] Si veda la guida dell'Information Commissioner's Office, anche detta ICO, pubblicata al link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection regulation-gdpr/personal-data-breaches.

- Una descrizione delle misure di sicurezza tecniche e organizzative identificate per i vari trattamenti.
- L'identificazione degli autorizzati ai vari trattamenti.
- Una valutazione d'impatto sulla protezione dei dati.

Una volta in possesso di tutte le informazioni elencate è possibile procedere alla fase successiva.

5.1 AVVIO DELLA GESTIONE DELLA VIOLAZIONE

La violazione dei dati personali come sopra definita e descritta si realizza a seguito del verificarsi di uno o più eventi che abbiano portato alla divulgazione (intenzionale o non), alla distruzione, alla perdita, alla modifica o all'accesso non autorizzato ai dati personali trattati dal titolare.

Una volta appurata la violazione è necessario informare tempestivamente il:

- Titolare del trattamento
- Responsabile al trattamento
- DPO
- Privacy Manager
- Amministratore di sistema

Ricevuta l'informazione, il titolare del trattamento o un suo incaricato provvede a:

- Aprire la gestione della violazione, compilando il modulo "Notifica di data breach – violazione dei dati personali".
- Convocare tempestivamente i delegati interni di competenza, per inquadrare l'ambito del trattamento in cui si è verificata violazione.
- Stabilire le azioni immediate da eseguirsi, le priorità, le responsabilità e le tempistiche. Con specifico riferimento alla definizione delle priorità, va considerata la seguente scala:
    1) Priorità Alta: **dove si riscontri un rischio per i diritti e le libertà degli interessati elevato** è necessario provvedere a correzioni da attuare immediatamente per impedire ulteriori rischi.
    2) Priorità Media: **dove si riscontra rischio per i diritti e le libertà degli interessati medi** è necessario provvedere a correzioni da attuare velocemente perché possono evitare un aumento dei rischi.
    3) Priorità Bassa: **dove si riscontra rischio per i diritti e le libertà degli interessati basse,** l'azione di contrasto va eseguita dopo aver posto in essere le correzioni con priorità alta e media.
    4) Priorità nulla: **dove si riscontra rischio trascurabile per i diritti e le libertà dell'interessato**, non è necessaria alcuna azione.

Qualora il titolare del trattamento sospetti che la violazione relativa alla sicurezza delle informazioni sia attribuibile ad un atto fraudolento da parte di una persona (sia fisica che giuridica), il titolare del trattamento deve interpellare l'Autorità Giudiziaria competente – Polizia Postale – e deve interrompere qualsiasi attività che possa contaminare in qualsiasi modo gli elementi che potrebbero essere oggetto di indagini. Inoltre, le evidenze oggettive

(testimonianze, documenti, ecc.) atte a dimostrare la responsabilità della persona devono essere raccolte quanto prima e conservate a cura dello stesso titolare del trattamento, al fine di poter intraprendere un'eventuale azione legale (civile o penale) se necessario.

5.2 NOTIFICA DELLA VIOLAZIONE ALL'AUTORITÀ DI CONTROLLO

Come sopra specificato, nel caso di comprovata violazione dei dati personali, il titolare del trattamento notifica la violazione all'Autorità di Controllo competente – il Garante per la Protezione dei Dati Personali ex art. 153 D.lgs. 196/2003, a norma dell'art. 33 del Regolamento (UE) 2016/679, 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.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza 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 dei dati personali coinvolti.

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati 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.

Il Regolamento (UE) 2016/679 riconosce l'eventualità che non sempre sia possibile raccogliere tutte le informazioni necessarie in sole 72 ore al fine di comprendere esattamente cosa sia successo e su cosa sia necessario intervenire. Per tale ragione l'art. 33 permette al titolare del trattamento di riportare le informazioni richieste per fasi successive, senza ulteriore ingiustificato ritardo. In ogni caso, è necessario che il titolare del trattamento dia una priorità all'indagine, procedendo con risorse adeguate e con la dovuta urgenza. Si richiede, infatti, che il titolare del trattamento notifichi comunque la violazione nel momento in cui egli ne venga a conoscenza, e che inoltri le successive informazioni il prima possibile: si evidenzia che nel caso in cui vi sia già coscienza dell'impossibilità di comunicare le informazioni dettagliate come sopra evidenziate, è in ogni caso consigliabile spiegare all'Autorità di Controllo i motivi del ritardo, individuando un termine entro il quale si ritiene possibile poter comunicare le ulteriori informazioni[10].

Il titolare del trattamento, inoltre, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di Controllo di verificare il rispetto del presente articolo.

[10] Si veda la guida dell'Information Commissioner's Office, anche detta ICO, pubblicata al link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection regulation-gdpr/personal-data-breaches.

In tale sede, si ricorda che, nel caso si verifichi una data breach che colpisca interessati ubicati in Paesi Europei diversi, il Garante per la Protezione dei Dati Personali potrebbe non essere l'Autorità di Controllo capofila. Ciò significa, dunque, che parte della procedura di risposta ad un data breach deve essere finalizzata necessariamente a individuare quale delle Autorità di Controllo Europee sia quella capofila e competente a ricevere la notifica di data breach. A tal fine, per una guida completa finalizzata a determinare quale sia l'Autorità di Controllo capofila, si rinvia alle "Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento", emanate dal Working Party art. 29 Regolamento (UE) 2016/679[11].

5.3 COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Nel caso in cui sia probabile che la violazione possa comportare dei rischi elevati per i diritti degli interessati, il Regolamento (UE) 2016/679 prevede che il titolare debba informare gli interessati direttamente coinvolti senza ingiustificato ritardo, e dunque il prima possibile.

Se, infatti, la notifica all'Autorità di Controllo è obbligatoria ogni qual volta si verifichi un evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, la comunicazione all'interessato necessita, per la sua verificazione, l'identificazione di un rischio ulteriormente più alto di danno per i diritti e le libertà degli interessati. Per tali ragioni, il titolare del trattamento dovrà valutare la gravità, sia potenziale che reale, dell'impatto sugli individui quale risultanza della violazione, e la probabilità della sua verificazione. Nel caso in cui le conseguenze dell'impatto della violazione siano particolarmente gravose, il rischio è alto: in tali casi, il titolare del trattamento dovrà informare prontamente gli interessati coinvolti e colpiti dalla violazione, e ciò in modo particolare laddove vi sia la necessità di mitigare un rischio immediato di danno. Uno dei motivi principali, infatti, che determinano la necessità di provvedere alla comunicazione nei confronti degli interessati è quello di proteggerli dagli effetti del data breach.

6 RISPOSTA ALLA VIOLAZIONE DELLE PROTEZIONI DEI DATI PERSONALI

Oltre alle attività di monitoraggio, identificazione e notifica della violazione è necessario inoltre:

1. Che le attività di risposta siano coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine.
2. Che vengano condotte approfondite analisi per assicurare un'adeguata riposta e supporto alle eventuali attività di ripristino o compartimentazione della violazione
3. Che vengano eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per rimuovere le cause della violazione. L'evento che ha determinato la violazione del dato personale, inoltre, dovrà essere necessariamente tenuto conto nella successiva valutazione di impatto sulla protezione dei dati personali ai sensi dell'art. 35 Regolamento (UE) 2016/679.

[11] Si vedano sul punto le "*Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento*", WP 244.

7 ELENCO DEI DOCUMENTI ALLEGATI ALLA PROCEDURA E MODALITÀ DI CONSERVAZIONE

Documento	Responsabile conservazione	Luogo di conservazione	Tempo conservazione
Notifica di data breach – violazione dei dati personali	Titolare del trattamento	Protocollo Generale	Legato alle finalità istituzionali

COMUNE DI CITTADELLA

PROVINCIA DI PADOVA

Notifica di Data Breach – violazione dei dati personali

Il presente form può essere utilizzato dalle Organizzazioni che abbiano subito un data breach e necessitino pertanto di segnalarlo al Garante per la Protezione dei Dati Personali. Si chiede cortesemente che nessuno dei dati personali coinvolti nel data breach sia riportato nella compilazione del presente modulo: ad esempio, non inserite i nominativi degli interessati colpiti da data breach.

Prima di procedere alla compilazione del modulo per la notifica di data breach, è necessario assicurarsi che le informazioni in possesso siano il più accurate e dettagliate possibili.

Nel caso in cui abbiate già avuto contatti con il Garante per la Protezione dei Dati Personali in merito al data breach di cui all'oggetto della presente, Vi preghiamo di indicare il nominativo del funzionario intervenuto:

Tipologia di segnalazione

☐ Prima segnalazione

☐ Segnalazione integrativa

(nel solo caso di segnalazione integrativa) numero di protocollo Garante:

Motivazioni della notifica – a seguito della

☐ Ritengo che l'incidente comporti un rischio per i diritti e le libertà degli interessati coinvolti e pertanto è necessaria la notifica all'Autorità di Controllo

☐ Non ritengo che l'incidente comporti un rischio per i diritti e le libertà degli interessati coinvolti, tuttavia preferisco essere vigile ed attento rispetto al problema

☐ Non sono sicuro che l'incidente comporti un rischio per i diritti e le libertà degli interessati coinvolti

In merito alla violazione dei dati personali

Che cosa è successo?

Vi preghiamo in tale sede di riferirci tutto ciò che sapete rispetto a quanto accaduto, che cosa è successo e come è successo

Il data breach è stato causato da un incidente informatico?

☐ Sì

☐ No

☐ Non lo so

Come siete venuti a conoscenza della violazione?

Quando siete venuti a conoscenza della violazione?

Data: **Errore. L'origine riferimento non è stata trovata.**

Ora: **Errore. L'origine riferimento non è stata trovata.**

Categorie di dati personali coinvolti nel data breach (si prega di selezionare tutti quelli coinvolti)

☐ Dati che rivelano l'origine razziale o l'etnia

☐ Opinioni politiche

☐ Convinzioni religiose o filosofiche

☐ Appartenenza sindacale

☐ Dati relativi alla vita sessuale

☐ Dati relativi all'orientamento sessuale

☐ Dati relativi al cambio di sesso

☐ Dati relativi allo stato di salute

☐ Dati personali comunemente identificativi, es. nome, dati di contatto

☐ Dati di identificazione, es. username, passwords

☐ Dati economici e finanziari, es. numero di carta di credito, dettagli bancari

☐ Documenti ufficiali, es. numero di patente

☐ Dati relativi all'ubicazione, geolocalizzazione

☐ Dati genetici o biometrici

☐ Dati relativi a condanne penali e reati

☐ Non sono ancora a conoscenza di quali siano le categorie di dati personali coinvolte

☐ Altri (si prega di specificare di seguito)

Numero di dati personali coinvolti?

Quanti interessati potrebbero essere colpiti dal data breach?

Categorie di interessati colpiti (si prega di selezionare tutti quelli coinvolti)

☐ Dipendenti o soggetti equiparabili per rapporto lavorativo

☐ Utenti

☐ Soggetti iscritti

☐ Studenti

☐ Clienti o eventuali clienti

☐ Pazienti

☐ Adulti vulnerabili

☐ Non sono ancora a conoscenza di quali siano le categorie interessati colpiti

☐ Altri (si prega di specificare di seguito)

Conseguenze potenziali del data breach

Vi preghiamo di descrivere il possibile impatto della violazione sugli interessati coinvolti, quale conseguenza del data breach. Vi preghiamo di comunicare soprattutto se vi siano già stati effettivi danni per gli interessati

Quali sono le probabilità che gli interessati possano essere colpiti da conseguenze significative quale risultato del data breach?

☐ Molto probabile

☐ Probabile

☐ Né probabile né improbabile

☐ Improbabile

☐ Molto improbabile

☐ Non è ancora possibile stabilire la probabilità

Vi preghiamo di darci dei dettagli in merito alla risposta selezionata:

(Solamente nel caso di incidente informatico) è stata colpita la riservatezza, l'integrità e/o la disponibilità del Vostro sistema informativo?

☐ Sì

☐ No

☐ Non lo so

(Solamente nel caso di incidente informatico) Impatto sulla Vostra Organizzazione

☐ Alto – avete perso la capacità di erogare servizi essenziali per i Vostri utenti

☐ Medio – avete perso la capacità di erogare servizi fondamentali solo ad alcuni dei Vostri utenti

☐ Basso – Non vi è stata alcuna perdita di efficienza, o vi è stata una limitata perdita di efficienza, e siete comunque in gradi di erogare tutti i servizi essenziali ai Vostri utenti

☐ Non è possibile stabilirlo al momento

(Solamente nel caso di incidente informatico) Tempo di ripristino

☐ Regolare – potete stabilire il Vostro tempo di ripristino, mediante le risorse già a disposizione

☐ Integrativo – potete stabilire il Vostro tempo di ripristino con risorse aggiuntive

☐ Esteso – non potete stabilire il Vostro tempo di ripristino, e necessitate di risorse aggiuntive

☐ Non ripristinabile – il ripristino a seguito dell'incidente non è possibile, ad esempio il backup non può essere recuperato

☐ Completato – il ripristino è già stato completato

☐ Non è ancora possibile stabilirlo

I membri dello staff coinvolti nel data breach avevano ricevuto formazione in materia di tutela del dato personale negli ultimi due anni?

☐ Sì

☐ No

☐ Non lo so

(Solamente in caso di prima segnalazione) Nel caso in cui vi siano stati ritardi nella segnalazione della presente violazione, Vi preghiamo di spiegarne le motivazioni

Agire

Descrivete le azioni che avete posto in essere, o che vi siete prefissi di porre in essere, a seguito del data breach

Incluse, nel caso in cui sia possibile individuarle, le azioni che avete posto in essere per correggere ed eliminare il problema, e per mitigare gli effetti dannosi, ad esempio la conferma che i dati inoltrati per errore siano stati distrutti dal destinatario, il cambio di password, la pianificazione di una formazione specifica in materia di sicurezza dell'informazione.

(Solamente in caso di segnalazione integrativa) Descrivete ogni step da Voi intrapreso al fine di prevenire ogni reiterazione, e quando vi aspettate che tali step siano completati

Avete informato gli interessati coinvolti del data breach?

☐ Sì, abbiamo provveduto a comunicare la violazione agli interessati colpiti

☐ Stiamo per procedere con la comunicazione, o stiamo già procedendo alla comunicazione

☐ No, non abbiamo provveduto alla comunicazione, ma gli interessati ne sono già a conoscenza

☐ No, ma abbiamo deciso di procedere con la comunicazione

☐ No, abbiamo deciso di non procedere con la comunicazione

☐ Non abbiamo ancora deciso se procedere o meno con la comunicazione

☐ Altro (Vi preghiamo di descrivere nel dettaglio tale situazione)

Avete comunicato, o state per comunicare ad altre Organizzazioni la violazione?

Ad esempio alla Polizia Postale o ad altre Autorità di Controllo. In questo caso è necessario che indichiate tali destinatari per permettere al Garante di contattarli

☐ Sì

☐ No

☐ Non lo so

Nel caso in cui abbiate risposto Sì, Vi preghiamo di specificare

I Vostri dati

Organizzazione (Titolare del trattamento) nominativo

Indirizzo/sede legale

Persona fisica che provvede alla presente segnalazione

Nel caso in cui vi sia la necessità di contattarVi direttamente

Nome: **Errore. L'origine riferimento non è stata trovata.**

E-mail: **Errore. L'origine riferimento non è stata trovata.**

Telefono: **Errore. L'origine riferimento non è stata trovata.**

Responsabile per la protezione dei dati – DPO/RPD

O, in alternativa, il soggetto che si occupa degli adempimenti relativi alla tutela del dato personale all'interno della Vostra Organizzazione

☐ Stesso soggetto sopra indicato

Nome: **Errore. L'origine riferimento non è stata trovata.**

E-mail: **Errore. L'origine riferimento non è stata trovata.**

Telefono: **Errore. L'origine riferimento non è stata trovata.**

Inoltrare la notifica di data breach

La notifica va trasmessa al Garante per la Protezione dei Dati Personali, inviandola all'indirizzo: **protocollo@pec.gpdp.it**

Nel caso di segnalazione integrativa, sarà necessario seguire le indicazioni date dal Garante stesso nella prima risposta inviataVi, con indicazione del numero di protocollo del fascicolo.

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

Proposta N. 2019 / 1380
SERVIZIO CED

OGGETTO: ARTICOLI 33 E 34 DEL REGOLAMENTO (UE) 2016/679. ADOZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI ("DATA BREACH")

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Ai sensi dell'art. 49 del D. Lgs 18.08.2000 n° 267, si esprime sulla proposta di deliberazione in oggetto parere *FAVOREVOLE* in ordine alla sola regolarità tecnica, dando atto che la presente proposta:

non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente;

Lì, 12/07/2019

IL DIRIGENTE
NICHELE EMANUELE
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

Proposta N. 2019 / 1380
SERVIZIO CED

OGGETTO: ARTICOLI 33 E 34 DEL REGOLAMENTO (UE) 2016/679. ADOZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI ("DATA BREACH")

PARERE IN ORDINE ALLA REGOLARITA' CONTABILE

Parere del Responsabile di Ragioneria in ordine alla regolarità contabile (art. 49, comma 1, D. Lgs 18.08.2000 n. 267, così come sostituito dall'art. 3 del D.L. 174/2012) :

parere *FAVOREVOLE*

Lì, 12/07/2019

IL DIRIGENTE
SARTORE CARLO
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)