Originale informatico sottoscritto con firma digitale ai sensi del D.Lgs. 07/03/2005, n. 82

Deliberazione **Nr. 115**
in data **03-12-2020**

COMUNE DI LUGO DI VICENZA

PROVINCIA DI VICENZA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) AI SENSI DEL REGOLAMENTO (UE) N.679/2016

Il giorno **tre** del mese di **dicembre** dell'anno **duemilaventi** si è riunita in videoconferenza la Giunta Comunale attraverso la piattaforma web "jitsi", sotto la presidenza del Sindaco **Loris Dalla Costa.**

Tutti i partecipanti risultano connessi e riconoscibili sia in audio che in video, come stabilito dall'art. 5 del regolamento per il funzionamento della giunta comunale approvato con delibera di GC n.9 del 06/02/2020 e modificato con delibera di G.C. n.35 del 26/03/2020.

All'inizio della trattazione della presente deliberazione, risultano presenti:

Cognome e Nome	Presente / Assente
Dalla Costa Loris	P
Rabito Roberto	P
Dal Ponte Giovanni	P
Ranzolin Emanuela	P
Carollo Stefania	P

Il Presidente, riconosciuta legale l'adunanza, invita i presenti a prendere in esame la proposta di deliberazione avente l'oggetto sopra riportato.

Assiste alla seduta il Segretario Comunale **Giuseppe Taibi.**

PROPOSTA DI DELIBERAZIONE DI GIUNTA COMUNALE
N. 115 DEL 24-11-2020

La sottoscritta Pornaro Chiara, responsabile dell'AREA AMMINISTRATIVA del Comune di Lugo di Vicenza, ha redatto la seguente proposta di deliberazione avente ad oggetto:

"APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) AI SENSI DEL REGOLAMENTO (UE) N.679/2016"

Rilevato che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

Considerato che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

Tenuto presente che tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

Dato atto che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

Rilevato che, con il GDPR, è stato richiesto agli Stati membri:

- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

Visto il D.Lgs. 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

Dato atto che il GDPR introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate;

Dato atto che la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare 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.

Tenuto presente che la violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR;

Dato atto che, 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, e che tale comunicazione deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali, contenendo obbligatoriamente i seguenti contenuti minimi:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili 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 e anche, se del caso, per attenuarne i possibili effetti negativi.

Rilevato che, per quanto sopra, è necessario istituire:

1. una Procedura *data breach*
2. un registro interno *data breach*, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere i seguenti dati:
   - i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
   - gli effetti e le conseguenze della violazione;
   - i provvedimenti adottati per porvi rimedio;
   - il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);

Dato atto che la Procedura *data breach,* avente lo scopo di indicare le modalità di gestione del *data breach, garantisce* la realizzabilità tecnica e la sostenibilità organizzativa;

Dato atto che responsabili del procedimento sono i Responsabile di Area, i quali, con riferimento ai propri settori di attività dovranno garantire la massima diffusione interna ed esterna e la massima conoscibilità delle azioni da intraprendere e dei comportamenti da adottare in caso di *data breach*;

Visti:

- il D.Lgs. 267/2000, laLegge 241/1990, il D.Lgs. 196/2003, la Legge 190/2012, il D.Lgs. 33/2013 e loro successive modifiche ed integrazioni;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla *"portabilità dei dati"* - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento *"possa presentare un rischio elevato"* ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto Comunale;
- Regolamento sull'organizzazione degli uffici e dei servizi;
- Codice di comportamento interno dell'Ente;
- Circolari e direttive del RPC;

PROPONE

1) di approvare la Procedura per la gestione di ***data breach*** ai sensi del Regolamento (UE) n. 679/2016, allegata alla presente, per formarne parte integrante e sostanziale;

2) di dare atto che responsabili del procedimento sono i Responsabile di Area, i quali, con riferimento ai propri settori di attività dovranno garantire la massima diffusione interna ed esterna e la massima conoscibilità delle azioni da intraprendere e dei comportamenti da adottare in caso di data breach;

3) di demandare la concreta attuazione delle misure regolamentari minime contenute nelle disposizioni operative al personale operante all'interno dell'Ente nelle sue articolazioni gerarchiche e secondo le loro rispettive funzioni e competenze;

4) di disporre che al presente provvedimento venga assicurata:
   a) la pubblicità legale con pubblicazione all'Albo on line del Comune di Lugo di Vicenza;

b) la trasparenza amministrativa mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione “Amministrazione trasparente”, sezione di primo livello “Disposizioni generali" sezione di secondo livello “Atti generali”;

5) di dare atto che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell’art. 5 comma 2 D.Lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto;

6) di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvenga nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti;

7) di inviare il presente provvedimento a tutti il personale dipendente del Comune di Lugo di Vicenza.

Di attribuire alla stessa il carattere dell’immediata eseguibilità stante l’urgenza di provvedere.

--- *fine proposta* ---

LA GIUNTA COMUNALE

VISTA la suestesa proposta di deliberazione accompagnata dai prescritti pareri espressi ai sensi dell’art. 49, comma 1, del D.Lgs. 267/2000, come sotto riportati.

Con voti unanimi favorevoli resi nelle forme di legge;

DELIBERA

di approvare la proposta in oggetto.

Successivamente, rilevata l’urgenza di provvedere, con successiva e separata votazione unanime favorevole, resa nei modi di legge;

DELIBERA

di dichiarare il presenta atto immediatamente eseguibile ai sensi dell’art. 134, comma 4, del D.Lgs. 267/2000.

IL PRESIDENTE - Loris Dalla Costa *(firmato digitalmente)*

IL SEGRETARIO COMUNALE - Giuseppe Taibi *(firmato digitalmente)*

PARERI ESPRESSI AI SENSI DELL'ART. 49, COMMA 1, DEL D.LGS. 267/2000, SULLA PROPOSTA DI DELIBERAZIONE N. 115 DEL 24-11-2020:

Parere Favorevole di REGOLARITA' TECNICA - AMM reso da Pornaro Chiara - Responsabile Area Amministrativa in data 01-12-2020.
Parere Visto di REGOLARITA' CONTABILE reso da Ranzolin Paola - Responsabile Area Finanziaria in data 01-12-2020.

COMUNE DI LUGO DI VICENZA

PROVINCIA DI VICENZA

PROCEDURA
PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH)*
AI SENSI DEL GDPR (REGOLAMENTO EUROPEO 679/2016)

Approvata con deliberazione di Giunta Municipale n. _____ del _____

Sommario

Premessa 3

1. Normativa e documenti di riferimento 3

2. Definizione di violazione dei dati: 4

2.1 Classificazione delle violazioni: 4

2.2 Tipologie di violazioni 4

2.3 Esempi di eventi che possono generare violazione di dati 4

2.3.1 Eventi riguardanti trattamenti elettronici: 4

2.3.2 Eventi riguardanti trattamenti cartacei 5

3. Notifica della violazione all'autorità di controllo 6

3.1 Quando è richiesta la notifica 6

3.2. Quando non è richiesta la notifica 6

4. Contitolari del trattamento 7

5. Responsabile del trattamento 7

6. Responsabile della protezione dati (RPD) 7

7. Contenuti della notifica: informazioni obbligatorie da fornire all'autorità di controllo 7

8. Comunicazione all'interessato 8

8.1 Contenuto della comunicazione 8

8.2 Modalità della comunicazione 8

8.3 Quando la comunicazione non deve essere effettuata 8

8.4 Quando la comunicazione va sempre effettuata 9

9. Valutazione del rischio 9

10. Registro delle violazioni 11

Allegato 1 - Potenziale violazione di dati personali - Stima della violazione di sicurezza e adempimenti conseguenti 12

Premessa

Il Regolamento Europeo sulla protezione dei dati n. 679/2016 (di seguito "GDPR"), entrato in vigore definitivamente il 25 maggio 2018, introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (*data breach*) e di rendere nota la violazione stessa alle persone fisiche interessate.

La violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR.

Il GDPR impone al titolare di disporre le misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati al fine di proteggerli dalle violazioni sopra descritte.

Il presente documento si prefigge lo scopo di indicare le modalità di gestione del *data breach* garantendone la realizzabilità tecnica e la sostenibilità organizzativa.

La presente procedura viene approvata dalla Giunta Municipale con propria deliberazione; compete allo stesso organo definire eventuali modifiche o integrazioni.

Al fine di garantirne la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di *data breach* la presente viene comunicata a tutti i dipendenti dell'Ente dopo la sua approvazione e resa disponibile sul sito web istituzionale nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy".

1. Normativa e documenti di riferimento

La presente procedura viene adottata sulla base delle disposizioni contenute nei seguenti provvedimenti:

- **Regolamento (UE) n. 679/2016;**
- **Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;**
- **Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;**
- **Linee-guida sul diritto alla *"portabilità dei dati"* - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;**
- **Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;**
- **Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento *"possa presentare un rischio elevato"* ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;**
- **Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;**
- **Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;**
- **Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (*data breach notification*) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;**
- **Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;**
- **Statuto Comunale;**
- **Regolamento sull'organizzazione degli uffici e dei servizi;**

- **Codice di comportamento interno dell'Ente;**
- **Circolari e direttive del RPC;**

2. Definizione di violazione dei dati:

2.1 Classificazione delle violazioni:

Le violazioni si classificano nel seguente modo:

- **violazione della riservatezza: in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;**
- **violazione dell'integrità : in caso di modifica non autorizzata o accidentale dei dati personali;**
- **violazione della disponibilità: in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.**

La violazione può riguardare la riservatezza, l'integrità, la disponibilità dei dati personali o qualsiasi combinazione delle stesse.

Al fine di adottare le corrette procedure di segnalazione è di fondamentale importanza sapere identificare una violazione, saperne valutare la natura e le potenziali conseguenze negative.

Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi, ecc.).

2.2 Tipologie di violazioni

All'interno della classificazione sopra indicata, quindi, si possono avere le seguenti tipologie di violazione dei dati personali:

- **Distruzione: Indisponibilità definitiva di dati personali con impossibilità di ripristino degli stessi. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati.**
- **Perdita: Perdita del supporto fisico di memorizzazione dei dati derivante da privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita, può riguardare anche copie od originali dei supporti contenenti i dati personali dei soggetti interessati, ed anche se temporanea può essere potenzialmente dannosa.**
- **Modifica: Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.**
- **Rivelazione: Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.**
- **Accesso: Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.**

2.3 Esempi di eventi che possono generare violazione di dati

Al fine di facilitare l'individuazione di una possibile violazione, vengono di seguito indicati in modo esemplificativo e non esaustivo, una serie di possibili eventi che potenzialmente possono generare violazioni dei dati personali. Pertanto si può essere in presenza di un *data breach* anche nel caso di un evento non compreso nell'elenco di seguito riportato, di contro il verificarsi di uno degli eventi che seguono non costituisce condizione sufficiente per stabilire l'effettivo *data breach.* Il titolare deve infatti procedere sempre alle opportune valutazioni.

2.3.1 Eventi riguardanti trattamenti elettronici:

a) Eventi accidentali: Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali dei clienti (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- **esecuzione erronea di comandi e/o procedure per distrazione: ad esempio pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici;**

erroneo invio di informazioni a enti esterni al Comune, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato ecc.

- **rottura delle componenti HW: a titolo di esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.**
- **malfunzionamenti software: ad esempio esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.**
- **visibilità errata di dati sul sito web dell'Ente: ad esempio visibilità di dati di altri utenti anche per casi di omonimia.**
- **fornitura dati a persona diversa dall'interessato: a titolo di esempio comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;**
- **guasti alla rete: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.**

b) Eventi dolosi: eventi dolosi causati da personale interno o soggetti esterni realizzati tramite: accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione; compromissione o rivelazione abusiva di credenziali di autenticazione; utilizzo di software malevolo. In tale casistica rientrano gli incidenti di sicurezza ICT che comportano la violazione dei dati personali quali:

- **furto: furto di supporti di memorizzazione e/o elaborazione contenenti dati personali dei clienti;**
- **truffa informatica esterna: tutti i casi di frodi realizzate da un soggetto esterno dell'Ente rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori. Ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi;**
- **appropriazione dei dati di carta di credito; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi dei clienti.**
- **truffa informatica interna: tutti i casi di frodi realizzate da personale interno all'Ente che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.**

2.3.2 Eventi riguardanti trattamenti cartacei

a) Eventi accidentali: Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali dei clienti dell'ente quali:

- **Distruzione accidentale di documenti: ad esempio incendio/ allagamento dei locali dove sono presenti archivi cartacei, causati da eventi fortuiti e non dolosi presso le sedi dell'ente e dei locali, degli *outsourcers* di archiviazione contratti, dei collaboratori cessati dai quali si attende la restituzione della documentazione contrattuale;**
- **Distruzione per errore di documenti originali, senza eventuale copia, da parte di dipendenti interni, di collaboratori esterni;**
- **Smarrimento di documenti: ad esempio perdita di documenti contenenti dati dei cittadini, degli *outsourcers* (es. archiviazione contratti).**
- **Fornitura involontaria di dati a persona diversa dal contraente: ad esempio invio lettera ad un ente senza mandato, gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal titolare della linea non delegato, comunicazione di dati dal subentrato al subentrante e viceversa, invio/visualizzazione di fatture a soggetti diversi dagli autorizzati.**

b) **Eventi dolosi: Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati attraverso accessi non autorizzati nell'ambito di trattamenti effettuati su archivi cartacei di dati personali del Comune quali:**
   - **Distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati dell'utenza; accesso non autorizzato da parte di terzi ad archivi interni della Società e distruzione volontaria di documenti contenenti dati dell'utenza.**
   - **Accesso non autorizzato: ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ente, dei collaboratori esterni. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.**
   - **Furto (cartacei): Furto da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.**

3. Notifica della violazione all'autorità di controllo

3.1 Quando è richiesta la notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che la valutazione della violazione non evidenzi rischi per i diritti e le libertà delle persone fisiche. Ai fini di una stima attendibile del pregiudizio patito dall'interessato, si fa riferimento a quanto previsto dal paragrafo 9.1.

Il titolare del trattamento viene considerato "a conoscenza" della violazione nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione di dati personali.

Nei casi in cui la violazione non sia evidente e chiara il titolare è tenuto ad attivare tempestivamente le indagini finalizzate a valutare se l'incidente abbia causato una effettiva violazione di dati personali, ad adottare le dovute misure correttive e ad effettuare la notifica, se ritenuta necessaria.

La notifica all'autorità di controllo effettuata oltre le 72 ore, deve essere corredata dai motivi del ritardo.

Ogni singola violazione costituisce un incidente segnalabile con rispettiva notifica; fa eccezione il caso della notifica "cumulativa" da utilizzare in presenza di violazioni multiple riguardanti il medesimo tipo di dati personali violati nel medesimo modo ed in un lasso di tempo relativamente breve.

Contrariamente, diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, costituiscono separate notifiche per ogni violazione conformemente all'articolo 33.

L'articolo 33, paragrafo 4, afferma 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

Il titolare quindi, a seconda della natura e delle complessità della violazione, può effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente.

In questi casi il titolare provvede tempestivamente (entro le 72 ore) alla notifica all'autorità riservandosi di fornire informazioni supplementari in un secondo momento, si procede pertanto ad una notifica per fasi.

Se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento informa l'autorità di controllo.

L'incidente, in questo caso, viene registrato come un evento che non costituisce una violazione.

3.2. Quando non è richiesta la notifica

Quando dalla valutazione risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche il titolare non procede né alla notifica all'autorità di controllo né ad informare la persona interessata.

Nel caso in cui lo stato di assenza di un rischio probabile ai diritti ed alle libertà delle persone fisiche cambi nel corso del tempo si procede alla rivalutazione del rischio al fine di verificare se i nuovi elementi emersi rientrino nell'obbligo di notifica.

4. Contitolari del trattamento

In caso di presenza di contitolari del trattamento, il rispetto agli obblighi di notifica delle violazioni previsti dal GDPR, si fa rinvio agli accordi contrattuali che dovranno obbligatoriamente contenere l'indicazione del titolare responsabile delle violazioni e della eventuale notifica all'autorità di controllo.

5. Responsabile del trattamento

Il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi in materia di notifica delle violazioni.

Il contratto, o altro atto giuridico, che disciplina il rapporto tra il titolare ed il responsabile del trattamento deve contenere la seguente previsione "Il responsabile del trattamento assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento

Se il responsabile del trattamento viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, deve notificarla al titolare del trattamento senza ingiustificato ritardo e comunque non oltre le 24 ore.

La valutazione del rischio derivante dalla violazione spetta al titolare del trattamento nel momento in cui viene a conoscenza della violazione; in capo al responsabile del trattamento insiste esclusivamente l'obbligo di verificare l'esistenza di una violazione e di notificarla tempestivamente al titolare del trattamento nei tempi sopra indicati.

In considerazione del fatto che ai sensi del GDPR la responsabilità legale della notifica rimane sempre in capo al titolare del trattamento, il responsabile del trattamento può effettuare la notifica della violazione per conto del titolare esclusivamente nel caso in cui quest'ultimo gli abbia conferito apposita autorizzazione e/o nel caso in cui tale modalità sia espressamente prevista negli accordi contrattuali tra i due soggetti.

In caso contrario è fatto obbligo al responsabile del trattamento di informare il titolare, nelle modalità e nei tempi di cui sopra, di ogni potenziale evento di *data breach.*

La segnalazione può essere trasmessa via PEC all'indirizzo lugodivicenza.vi@cert.ip-veneto.net o via e-mail all'indirizzo info@comune.lugo.vi.it

Delle seguenti prescrizioni è fatta apposita menzione nel contratto, o altro atto giuridico, che disciplina il rapporto tra il titolare ed il responsabile del trattamento.

6. Responsabile della protezione dati (RPD)

Il Responsabile della Protezione dati (di seguito "RPD") fornisce consulenza e informazioni al titolare del trattamento e/o al responsabile del trattamento in merito alla valutazione della necessità di notificare una violazione. L'RPD coopera inoltre con l'autorità di controllo e funge da punto di contatto per l'autorità di controllo e per gli eventuali interessati.

Il RPD viene informato tempestivamente dell'esistenza di una violazione e viene coinvolto nell'intera gestione delle violazioni, nonché nel processo di notifica.

Il RPD, quindi, svolge un ruolo di assistenza nella prevenzione delle violazioni, fornisce consulenza e monitora il rispetto delle norme durante il processo di gestione della violazione e assiste l'Ente nell'eventualità di successive indagini da parte dell'autorità di controllo.

Il RPD, inoltre, su richiesta del titolare del trattamento, esprime pareri in merito alla struttura, all'impostazione, all'amministrazione ed alla conservazione della documentazione relativa al registro delle violazioni.

7. Contenuti della notifica: informazioni obbligatorie da fornire all'autorità di controllo

La notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- **descrizione della natura della violazione dei dati personali (compresi, ove possibile, le categorie e il numero degli interessati (persone fisiche i cui dati personali sono stati oggetto di violazione) e le registrazioni dei dati personali in questione (le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni di cui il titolare del trattamento può disporre, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.) ;**
- **comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;**
- **descrizione delle probabili conseguenze della violazione dei dati personali;**
- **descrizione delle misure adottate o da adottare 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.**

L'impossibilità da parte del titolare di disporre di informazioni precise (ad esempio il numero esatto di interessati coinvolti) non costituisce un ostacolo alla notifica tempestiva delle violazioni; in questo caso la comunicazione deve contenere un'approssimazione sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte.
Le informazioni sopra indicate costituiscono il contenuto minimo della notifica, è facoltà del titolare del trattamento, qualora lo ritenga necessario, fornire ulteriori informazioni.

8. Comunicazione all'interessato
Ai sensi dell'articolo 34, paragrafo 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".

8.1 Contenuto della comunicazione
La comunicazione di una violazione agli interessati deve avvenire senza ingiustificato ritardo e, deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali e deve contenere obbligatoriamente i seguenti contenuti minimi:

- **il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;**
- **una descrizione delle probabili 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 e anche, se del caso, per attenuarne i possibili effetti negativi.**

Il Responsabile di area cui fa capo il dato violato od anche più responsabili congiuntamente con il coordinamento del Segretario Comunale, qualora il dato faccia capo a più aree, predispone e invia la notifica della violazione all'autorità di controllo utilizzando il modello messo a disposizione sul sito del Garante della Privacy all'indirizzo https://www.garanteprivacy.it e invia il tutto tramite pec all'indirizzo protocollo@pec.gpdp.it;

8.2 Modalità della comunicazione
La violazione va comunicata direttamente agli interessati coinvolti.
Nel caso la comunicazione diretta non risulta percorribile si procede ad una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c); la misura più efficace, valutata la fattispecie concreta, viene stabilita dal titolare.
Il titolare, può contattare l'autorità di controllo per chiedere indicazioni ed orientamenti in merito all'opportunità di informare gli interessati sulla violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli. Qualora il titolare non sia in possesso di dati sufficienti per contattare l'interessato procede ad informarlo non appena sia ragionevolmente possibile (ad esempio può accadere che il titolare entra in possesso di dati necessari per contattare l'interessato nel momento in cui lo stesso esercita il proprio diritto di accesso ai dati ai sensi dell'articolo 15).

8.3 Quando la comunicazione non deve essere effettuata

La comunicazione agli interessati in caso di violazione dei dati non deve essere effettuata, ai sensi dell'articolo 34 paragrafo 3, se si verifica una delle seguenti tre condizioni:

- **il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione tali rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);**
- **subito dopo la violazione il titolare ha adottato una serie di misure che rendano improbabile l'elevato rischio posto ai diritti e alle libertà delle persone fisiche (es. l'immediata azione nei confronti del soggetto che ha avuto accesso ai dati personali in modo da inibirne qualsiasi utilizzo);**
- **contattare gli interessati richiede uno sforzo sproporzionato. In tale circostanza il titolare provvede ad effettuare una comunicazione pubblica o individua una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.**

Seppure la violazione inizialmente non rilevi necessità di una comunicazione all'interessato per l'assenza di rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe nel tempo subire delle variazioni, pertanto il titolare rivaluta il rischio e provvede all'eventuale comunicazione nelle modalità di cui sopra.

8.4 Quando la comunicazione va sempre effettuata

Il titolare provvede in qualunque caso alla comunicazione nel caso in cui questa venga richiesta direttamente all'autorità di controllo al fine di evitare da parte della stessa l'esercizio dei poteri sanzionatori.

9. Valutazione del rischio

I Responsabili di Area, venuti direttamente o indirettamente a conoscenza di una violazione dei dati personali che riguarda i dati detenuti per conto del titolare dal proprio settore, sono i soggetti competenti, per conto del titolare, all'effettuazione della valutazione.

Tutti i dipendenti comunali autorizzati a trattare dati, possono potenzialmente venire a conoscenza di un *data breach.* Al verificarsi di tale evento è fatto obbligo di avvisare tempestivamente il Responsabile di area in qualità di Designato dal Titolare al trattamento dati.

Il Responsabile del Servizio interessato dal *data breach* si avvale, altresì, della collaborazione del Segretario Comunale, il quale verifica immediatamente se la violazione coinvolge più aree ed in tal caso, previo coinvolgimento degli altri responsabili interessati, coordina le attività congiunte di valutazione della gravità del *data breach* e le decisioni in ordine alla necessità di notificare la violazione al garante e comunicarla all'interessato.

Non appena il titolare del trattamento viene a conoscenza di una violazione oltre a mettere in campo tutte le azioni necessarie a contenere l'incidente, valuta anche il rischio che potrebbe derivarne.

Il rischio viene valutato in base a criteri oggettivi; i considerando 75 e 76 stabiliscono che la valutazione deve tenere conto della probabilità e della gravità del rischio per i diritti e le libertà degli interessati.

La valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati (DPIA). La valutazione di impatto prende in considerazione infatti un evento ipotetico; nel caso invece di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione va concentrata esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

9.1 Stima di una violazione di sicurezza con riferimento ai diritti e alle libertà degli interessati

L'art. 33 del GDPR precisa che la notifica all'autorità di controllo deve essere svolta, secondo i tempi previsti, *"a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche"*.

Analogamente, ai sensi dell'art. 34, la comunicazione all'interessato è obbligatoria *"quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*, e nello specifico, non è richiesta se sono state messe in atto misure tecniche e

organizzative adeguate di protezione ovvero se i dati personali sono stati resi incomprensibili (ad es. tramite cifratura), oppure se è stato prontamente scongiurato il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Sulla base di quanto riportato dal Regolamento, risulta evidente come una corretta gestione delle violazioni di dati personali debba inevitabilmente:

- **tenere conto degli elementi tecnici e organizzativi che permettono di descrivere le circostanze della violazione stessa; quindi, anche sulla base di questi elementi**
- **svolgere una valutazione sui rischi che guidi la decisione di notificare/comunicare la violazione.**

Il Comune di Lugo di Vicenza ritiene che l'identificazione di un "criterio" o un metodo oggettivo e predefinito di valutazione sia una scelta in linea con il GDPR.

Il GDPR non specifica i metodi ritenuti adatti a valutare la presenza e l'entità dei rischi sui diritti e le libertà delle persone fisiche (lasciando pertanto una generale autonomia a ciascun Titolare del trattamento e il potere di scelta sulla modalità di approccio).

Per il principio di accountability (*responsabilizzazione)*, il Comune di Lugo di Vicenza intende formalizzare un metodo e dei criteri da utilizzare per la valutazione, facendo riferimento alle indicazioni dell'ENISA (European Union Agency for Network and Information Security), l'Agenzia europea per la sicurezza delle reti e dell'informazione.

Secondo il modello dell'ENISA, gli elementi centrali che devono essere presi in considerazione quando si valuta la gravità di una violazione di dati personali, sono:

- **Contesto del trattamento e tipologia di dati;**
- **Facilità di identificazione dell'individuo sulla base dei dati violati;**
- **Circostanze della violazione.**

Al fine di definire un punteggio al parametro relativo al contesto del trattamento, l'ENISA suggerisce di attribuire un punteggio di base utilizzando come criterio la classe di dati violati, regolando poi il punteggio sulla base dell'analisi di altri fattori di contesto.

Per quanto concerne la facilità di identificazione, la valutazione di questo parametro avviene in relazione a quattro livelli di identificabilità crescente, il cui valore sarà utilizzato come moltiplicatore sul punteggio di base del contesto del trattamento.

Infine, gli elementi relativi alle circostanze della violazione sono rappresentati dalle perdite di riservatezza (la cui entità varierà a seconda della portata della divulgazione), di integrità (di cui si valuterà quanto le alterazione possano essere pregiudizievoli per l'individuo), di disponibilità (in cui diventa rilevante il fatto che sia una perdita temporanea o permanente), oppure da circostanze di violazione provocata da intenzioni malevole (fattore che aumenta sempre la probabilità che i dati vengano utilizzati in modo dannoso).

CONTESTO DEL TRATTAMENTO	
Classe dei dati violati	*Punteggio di base **
Dati semplici	1
Dati comportamentali	2
Dati finanziari	3
Dati relativi a situazione di disagio economico-sociale	3,5

FACILITA' DI IDENTIFICAZIONE	
Livello di identificabilità	*Moltiplicatore*
Trascurabile	0,25
Limitato	0,5
Significativo	0,75
Massimo	1

CIRCOSTANZE DELLA VIOLAZIONE	
Circostanza	*Correzione*
Perdita di riservatezza	Da +0 a +0.50
Perdita di integrità	Da +0 a +0.50
Perdita di disponibilità	Da +0 a +0.50
Intenzioni malevole	+0.50

Dati particolari	4

**** Il punteggio di base rientrerà sempre in un valore da 1 a 4, a seconda delle successive correzioni. Ad es. a dati semplici potrebbe essere attribuito un punteggio di base = 4 qualora a causa di determinate caratteristiche dell'individuo l'informazione possa essere critica per la loro sicurezza personale o per le condizioni fisiche/psicologiche. Analogamente, anche a dati sensibili potrebbe essere attribuito un punteggio di base = 1, quando la natura dei dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo.***

Utilizzando i criteri suesposti, può essere calcolata quindi la gravità di una violazione di dati personali attraverso la formula:
Gravità = (Contesto x Facilità di identificazione) + Circostanze

valutando infine il risultato ottenuto secondo quanto riportato nella seguente tabella:

GRAVITA'	RISCHIO	DESCRIZIONE
Minore di 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc.)
Compreso tra 2 e 3	Medio	Gli interessati potranno incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc.)
Compreso tra 3 e 4	Alto	Gli interessati potranno incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, ecc.)
Maggiore di 4	Molto alto	Gli interessati potranno incontrare conseguenze significative o addirittura irreversibili che non potranno superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.)

Il Titolare del trattamento, mediante il responsabile del servizio interessato dal *data breach*, anche con l'ausilio del DPO, che viene immediatamente informato della violazione, prende nota della valutazione effettuata al momento del verificarsi della violazione, mediante apposito modulo (Allegato 1) e conserva la relazione all'interno del registro delle violazioni.

10. Registro delle violazioni

E' istituito un registro interno delle violazioni dove vengono annotate sia le violazioni non notificabili che quelle notificabili.

In ossequio al principio di responsabilizzazione di cui all'articolo 5 paragrafo 2, il titolare del trattamento conserva la documentazione di tutte le violazioni come stabilito all'articolo 33, paragrafo 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".

Il registro deve contenere i seguenti dati:

- **i dettagli relativi alla violazione (cause, fatti e dati personali interessati);**
- **gli effetti e le conseguenze della violazione;**
- **i provvedimenti adottati per porvi rimedio;**
- **il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);**

Il titolare conserva la documentazione in conformità dell'articolo 33, paragrafo 5, anche al fine di poter fornire prontamente le prove dall'autorità di controllo in caso di suo intervento.

COMUNE DI LUGO DI VICENZA

Il Responsabile Area _____ _____

nome e cognome

❑ **Vista la propria precedente comunicazione inviata al Sindaco e al DPO dell'Ente in data ……, prot. n. ……;**

❑ **Visti la relazione ed il parere del DPO dell'Ente in data ……, prot. n. ……;**

valuta la gravità della violazione calcolata attraverso la seguente formula:

(	**Contesto**	**x**	**Facilità di identificazione**	**)**	**+**	**Circostanze**	**=**	**Gravità**

dove :

al Contesto, in base alla classe dei dati violati, possono essere attribuiti i seguenti punteggi:

Classe dei dati violati	*Punteggio di base **
Dati semplici	1
Dati comportamentali	2
Dati finanziari	3
Dati relativi a situazione di disagio economico-sociale	3,5
Dati particolari	4

alla Facilità di identificazione, in base al livello di identificabilità, possono essere attribuiti i seguenti punteggi:

Livello di identificabilità	*Moltiplicatore*
Trascurabile	0,25
Limitato	0,5
Significativo	0,75
Massimo	1

alle Circostanze della violazione, in base alla circostanza, possono essere attribuiti i seguenti punteggi:

Circostanza	*Correzione*
Perdita di riservatezza	Da +0 a +0.50
Perdita di integrità	Da +0 a +0.50
Perdita di disponibilità	Da +0 a +0.50
Intenzioni malevole	+0.50

Quindi:

legenda

GRAVITA'	RISCHIO	DESCRIZIONE
Minore di 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc.)
Compreso tra 2 e 3	Medio	Gli interessati potranno incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc.)
Compreso tra 3 e 4	Alto	Gli interessati potranno incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, ecc.)
Maggiore di 4	Molto alto	Gli interessati potranno incontrare conseguenze significative o addirittura irreversibili che non potranno superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.)

ulteriori annotazioni:

Pertanto:

❑ **si ritiene che la violazione di dati personali possa avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.** ❑ **Si procede alla notifica della violazione all'Autorità di controllo.** **La notifica è stata effettuata il ……, prot. n. ……** ❑ **Si ritiene altresì che la violazione possa comportare un rischio elevato per i diritti delle persone per le seguenti motivazioni:**	❑ **si ritiene che la violazione di dati personali NON possa avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali;** ❑ **non si procede alla notifica della violazione all'Autorità di controllo;** ❑ **si procede all'inserimento della violazione nel registro delle violazioni.**

..... **Sarà necessaria, quindi, la comunicazione a tutti gli interessati che sarà effettuata con le seguenti modalità: …….** ❑ **Si procede all'inserimento della violazione nel registro delle violazioni.**	