Camera di Commercio, Industria, Artigianato e Agricoltura
BARI

DELIBERAZIONE N. 86 DEL 25.7.2019

OGGETTO: Approvazione procedura di gestione dei Data Breach ai sensi del Regolamento U.E. 2016/679

Il Presidente relaziona sull'argomento riferendo che, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*» (di seguito *GDPR*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Data Breach (artt. 33 e 34 *GDPR*).

Per Data Breach si intende "*una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.* (cfr. sito internet Garante della Privacy- pagina Violazioni di dati personali- Data Breach).

Le Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, adottate il 6 febbraio 2018, dal Gruppo di Lavoro di cui all'articolo 29 per la Protezione dei Dati prevedono che "*il regolamento impone al titolare del trattamento di attuare tutte le misure tecniche e organizzative di protezione adeguate per stabilire immediatamente se si è verificata una violazione e informare tempestivamente l'autorità di controllo e gli interessati. Afferma altresì che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate*".

A tal proposito, pertanto, in ossequio alla citata normativa, si rende necessaria l'approvazione da parte dell'Ente della "Procedura di gestione dei Data Breach" ai sensi del Regolamento UE 2016/679, di cui viene data lettura, come da bozza licenziata dal Gruppo di lavoro degli R.P.D. (di cui fa parte l'R.P.D. dell'Ente) delle Camere di Commercio istituito - con verbale del 13 novembre 2018 - da Unioncamere, allo scopo precipuo di adottare procedure condivise in materia di privacy - per tutti gli Enti camerali.

Il Presidente, pertanto, invita la Giunta camerale ad esprimersi su quanto sopra esposto.

LA GIUNTA

- sentita la *relazione del Presidente* ;
- vista la *Legge n. 580/1993* e s.m.i.;
- visto il vigente *Statuto* della Camera di Commercio di Bari;
- richiamata la *Deliberazione di Giunta n. 45 del 17.06.2019* con la quale, fra l'altro, è stato deciso che il Vice Segretario Generale Vicario, Avv. Vincenzo Pignataro, svolgerà le funzioni di Segretario Generale dell'Ente, fino alla data prevista dallo stesso provvedimento;
- visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento*

generale sulla protezione dei dati)» in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, che introduce la figura del Data Breach (artt. 33 e 34 GDPR);

- dato atto che per Data Breach si intende *"una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.* (cfr. sito internet Garante della Privacy- pagina Violazioni di dati personali- Data Breach).
- visti gli artt. 33 GDPR - " Notifica di una violazione dei dati personali all'autorità di controllo" e 34 GDPR - "Comunicazione di una violazione dei dati personali all'interessato";
- visto il Decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. n.101/2018;
- viste le Linee Guida in materia di notifica delle violazioni dei dati personali - WP250 rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, aggiornata al 06/02/2018;
- visti i Provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali e, in particolare, il Provvedimento n. 393 del 2 luglio 2015 - "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" e relativo Allegato 1 "Modello di comunicazione al Garante";
- vista la bozza di "Procedura di gestione dei Data Breach" ai sensi del Regolamento UE 2016/679 licenziata dal Gruppo di lavoro degli R.P.D. (di cui fa parte l'R.P.D. dell'Ente) delle Camere di Commercio istituito - con verbale del 13 novembre 2018 - da Unioncamere, allo scopo precipuo di adottare procedure condivise in materia di privacy per tutti gli Enti camerali, e ritenutala conforme alla normativa vigente;
- visto il parere favorevole reso dal Segretario Generale f.f. Avv. Vincenzo Pignataro in merito alla legittimità del provvedimento;
- A voti unanimi espressi ai sensi di legge

DELIBERA

per le motivazioni espresse in narrativa e qui da intendersi integralmente riportate:

1. di approvare la "Procedura di gestione dei Data Breach" che allegata al presente provvedimento ne forma parte integrante e sostanziale.

IL SEGRETARIO GENERALE f.f.
(Avv. Vincenzo Pignataro)

IL PRESIDENTE
(Dott. Alessandro Ambrosi)

CAMERA DI COMMERCIO
BARI

Camera di Commercio, Industria e Artigianato di Bari

SISTEMA DI GESTIONE DEI DATI PERSONALI
Procedura di gestione dei data breach
ai sensi del Regolamento UE 2016/679

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è descrivere compiti e responsabilità nel processo di gestione delle violazioni dei dati personali (c.d. *data breach*) nel rispetto delle disposizioni contenute nel Regolamento europeo n. 2016/679 (General Data Protection Regulation, di seguito GDPR).

Tale processo si sviluppa nelle seguenti fasi:

a) Rilevazione e inquadramento dell'incidente di sicurezza;

b) Messa in atto delle strategie di contenimento dei rischi e delle eventuali azioni correttive;

c) Svolgimento di ulteriore attività investigativa volta a individuare le conseguenze e/o i possibili rischi per i diritti e le libertà delle persone fisiche;

d) Eventuale notificazione del data breach all'Autorità Garante ai sensi dell'art. 33 GDPR e in conformità con le previsioni della WP 250 del 6 febbraio 2018;

e) Eventuale comunicazione agli Interessati coinvolti, quando la violazione dei dati personali presenta un rischio elevato per i loro diritti e libertà;

f) Registrazione dell'evento ai sensi dell'art. 33, par. 5, GDPR, al fine di documentare qualsiasi violazione dei dati personali comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Si tenga conto inoltre che la presente procedura si applica, per quanto compatibile, anche laddove:

1. la violazione coinvolga **dati trattati in regime di contitolarità**. Tuttavia, l'accordo di contitolarità può individuare specifiche ed ulteriori procedure e/o modalità di gestione dei data breach, determinando anche la responsabilità per l'adempimento agli obblighi di cui all'art. 33 GDPR e, in particolare, di notifica delle violazioni emerse;
2. la Camera di Commercio operi in **qualità di Responsabile Esterno del Trattamento**, ex art. 28 del GDPR. In tal caso, dovranno essere osservate anche le indicazioni ed istruzioni fornite dal Titolare nel relativo documento di nomina/designazione tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento. In tal caso, le fasi relative alla Notifica al Garante ed alla Comunicazione agli interessati sono di regola attuate dal Titolare del Trattamento, rispetto al quale il Responsabile esterno mantiene precisi obblighi di comunicazione e collaborazione.

La presente procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Responsabili delle Unità organizzative, funzionari o, comunque, referenti dei Settori/Uffici/Servizi della Camera di Commercio, nonché di tutto il personale dipendente autorizzato/designato al trattamento di dati personali.

La presente procedura è parte integrante del *Sistema Gestione Privacy* ed è pubblicata nella Intranet dell'Ente sulla cartella Comune.

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati personali":
   - art. 33 GDPR - Notifica di una violazione dei dati personali all'autorità di controllo;
   - art. 34 GDPR - Comunicazione di una violazione dei dati personali all'interessato.
2. Decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. n.101/2018
3. Linee Guida in materia di notifica delle violazioni dei dati personali - WP250 rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, aggiornata al 06/02/2018

4. Provvedimenti emessi dall'Autorità Garante e, in particolare, il Provvedimento n. 393 del 2 luglio 2015 – "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" e relativo Allegato 1 "Modello di comunicazione al Garante".

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice Privacy	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)
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
Interessato	La persona fisica cui si riferiscono i dati personali
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7 del GDPR)
DPO/ RPD	Data Protection Officer / Responsabile della protezione dei dati ai sensi dell'art. 37 del GDPR
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi dell'art. 4, punto 8 del GDPR
Referente Privacy	Persona nominata dalla CCIAA per coordinare le attività in ambito di privacy in carico all'Ente
Amministratore di Sistema Interno	Persona fisica incaricata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi comprese le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi
SG	Segretario Generale della CCIAA
Incidente di sicurezza	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi
Violazione dei dati (data breach)	L'incidente di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12 GDPR)

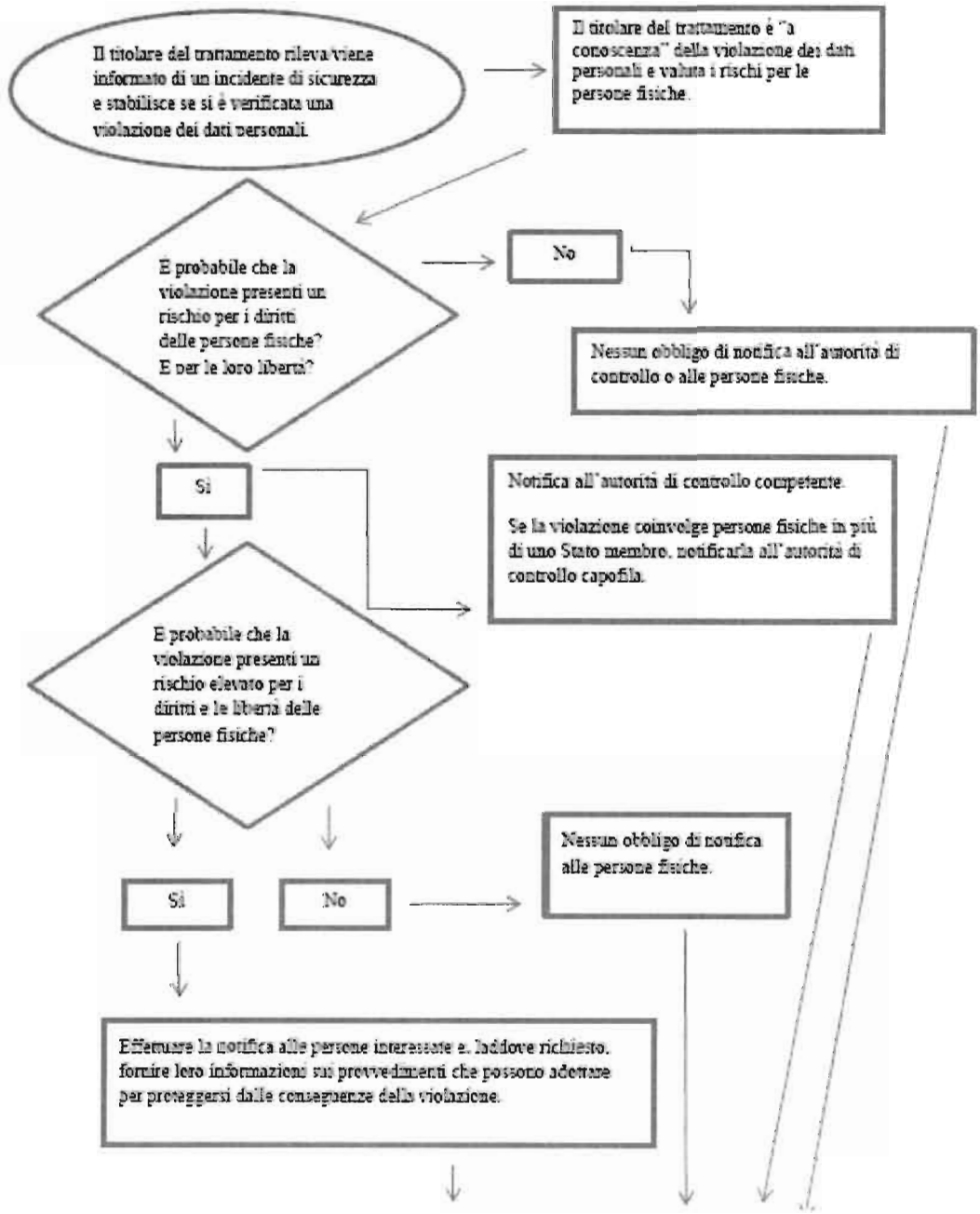
MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

FASI DEL PROCESSO

La gestione di un data breach può riassumersi nelle fasi di seguito rappresentate.

A. Diagramma di flusso che illustra gli obblighi di notifica



RILEVAZIONE E INQUADRAMENTO DELL'INCIDENTE DI SICUREZZA e ATTIVITA' DI REMEDIATION IMMEDIATE

La rilevazione di un incidente può avvenire da diverse fonti:

- **SEGNALAZIONE AUTOMATICA**: sistemi di segnalazione automatica (es. SIEM - *Security Information and Event Management*), come le violazioni derivanti da superamento dei sistemi di Firewall della Camera di Commercio (gestiti direttamente o tramite soggetti esterni), ovvero gestiti da InfoCamere.

- **SEGNALAZIONE INTERNA**: attività di monitoraggio degli eventi da parte del CED/Amministratori di sistema; comunicazione di: malfunzionamenti irrituali o blocco dei sistemi, furti, smarrimenti, intrusioni fisiche nei locali archivio.

- **SEGNALAZIONE ESTERNA**: da parte di Responsabili esterni nominati ai sensi dell'art. 28 GDPR, di fornitori esterni e/o altri consulenti nell'ambito dell'attività di monitoraggio, assistenza e manutenzione prestata a favore della CCIAA, ovvero di utenti dei servizi della Camera di Commercio e/o dei cittadini.

A tutti i soggetti che trattano dati per conto della CCIAA, quali Responsabili Esterni del Trattamento, devono essere imposto contrattualmente almeno i seguenti obblighi:

- comunicare al Referente contrattuale interno eventuali incidenti di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in essere e gli esiti delle stesse;
- fornire, in caso di necessità, anche attraverso il proprio RPD (ove nominato), la massima disponibilità e collaborazione per l'adempimento di tutti gli obblighi di cui agli artt. 32 e 36 GDPR.

Tutte le segnalazioni ricevute dall'Ente relative a incidenti di sicurezza devono essere inoltrate al Dirigente dell'Area interessata dall'evento. Quest'ultimo deve coinvolgere immediatamente il Referente Privacy interno.
Il Referente Privacy attiva il **Team di Primo Intervento** (di seguito **T1I**) composto da:

- Responsabile CED nominato con ordine di servizio del 18.10.2010 della società C.S.A. - società designata responsabile esterno del trattamento dei dati personali atteso lo svolgimento di servizi di gestione informatica e di assistenza manutentiva hardware e software dell'ente - ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente alla Camera di Commercio;
- referente delle Società in house (o esterne) coinvolte nell'incidente di sicurezza segnalato.

T1I deve assumere ogni informazione utile a inquadrare la tipologia dell'incidente e, conseguentemente, accertare se tale evento ha coinvolto o meno dati personali. In particolare, devono essere definiti:

1. il sistema, infrastruttura, applicazione, banca dati oggetto dell'incidente di sicurezza;
2. la tipologia dell'evento verificatosi (violazione della riservatezza/ dell'integrità /della disponibilità dei dati);
3. il volume dei dati e laddove possibile il numero degli interessati coinvolti;
4. le misure di sicurezza applicate;
5. le attività di remediation (azioni correttive) immediate;
6. le attività di remediation (azioni correttive) ipotizzabili e/o future affinché lo stesso evento non si ripeta più.

T1I pone in essere tutte le necessarie strategie di contenimento dei rischi e le eventuali azioni di *remediation* (azioni correttive) immediate, anche in collaborazione con il Dirigente dell'Area interessata dall'evento.

T1I relaziona sull'incidente di sicurezza e sulle misure di remediation ipotizzabili e/o future al Segretario Generale per ogni più opportuna decisione.

Nel caso in cui l'evento coinvolga dati personali, viene attivata la successiva fase che comporta lo svolgimento di attività investigativa volta ad individuare i possibili rischi per i diritti e le libertà delle persone fisiche, la segnalazione dell'evento al RPD e la costituzione del Team di secondo Intervento (di seguito T2I).

Ove il *data breach* interessi attività svolte dalla CCIAA in qualità di Responsabile Esterno del Trattamento, il Segretario Generale comunica l'evento al Titolare del trattamento.

SVOLGIMENTO DI ATTIVITÀ INVESTIGATIVA VOLTA AD INDIVIDUARE LE CONSEGUENZE E/O I POSSIBILI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

Dopo aver assunto tutte le informazioni di cui al punto precedente, ove l'incidente sia stato qualificato come *data breach*, il Referente Privacy segnala l'evento al **Team di Secondo intervento (T2I)** costituito da:

- RPD della Camera di Commercio;
- Dirigente dell'Area coinvolta nella violazione di dati;
- laddove presente, il referente dell'Ufficio legale interno;
- Responsabile CED nominato con ordine di servizio del 18.10.2010 della società C.S.A. - società designata responsabile esterno del trattamento dei dati personali atteso lo svolgimento di servizi di gestione informatica e di assistenza manutentiva hardware e software- ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente alla Camera di Commercio;
- Referente del Responsabile Esterno che ha realizzato/fornito il prodotto/servizio interessato dal *data breach* e/o il suo RPD (ove nominato).

T2I deve individuare le possibili conseguenze per i diritti e le libertà delle persone fisiche, valutarne la gravità e definire le misure da adottare nell'immediato in risposta all'emergenza al fine di contenere gli effetti negativi.

A tal fine:

a) ove disponibili sono raccolte, consolidate e/o approfondite le informazioni di cui al format per la comunicazione al Garante (***All. 1***);
b) successivamente, T2I effettuate le seguenti valutazioni circa:
    - la natura della violazione dei dati personali e, ove possibile, le categorie dei dati e il numero (anche solo) approssimativo degli interessati coinvolti (**c.d. gravità dell'accadimento**);
    - le possibili/probabili conseguenze della violazione accertata dei dati personali rispetto ai diritti ed alle libertà dell'interessato (ad esempio in termini di danno fisico, materiale o immateriale quali perdita del controllo dei dati personali o limitazione dei loro diritti; discriminazioni; furto o usurpazione d'identità; perdite finanziarie; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale; decifratura non autorizzata della pseudonimizzazione; qualsiasi altro danno economico o sociale) (**valutazione dell'entità dei possibili danni agli interessati**);
    - la valutazione dell'adeguatezza delle misure di sicurezza già implementate da parte del Titolare (o del Responsabile del trattamento) per porre rimedio alla violazione e per attenuare i possibili effetti negativi e/o probabili danni agli interessati.
    - le possibili azioni correttive da adottare nell'immediato al fine di contenere gli effetti negativi e minimizzare il possibile danno agli interessati.

Per la definizione dell'impatto sui diritti e le libertà degli interessati si fa riferimento ai livelli di rischio individuati dal manuale sulla sicurezza nel trattamento dei dati personali (rev. 12/2017) "ENISA" riportati nella seguente tabella:

GRAVITÀ	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 possono 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 possono incontrare conseguenze significative o addirittura irreversibili che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.)

Ad esito dell'analisi:

a) nel caso in cui risulti improbabile – anche in considerazione dell'adeguatezza delle misure correttive adottate – che la violazione presenti un rischio per i diritti e le libertà degli Interessati, il Referente Privacy provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD ed aggiorna il Registro dei Data breach come da format allegato (***All. 3***);
Copia del verbale deve essere inviata:
   - al RPD e;
   - al Segretario Generale che, se del caso, riferirà l'accaduto alla Giunta Camerale e adotterà ogni altro opportuna decisione di sua competenza.

b) nel caso risulti che la violazione possa comportare un rischio per i diritti e le libertà degli interessati, il Referente Privacy provvede a:
   - definire ed assegnare responsabilità e tempistiche per le azioni correttive individuate da T2I, anche verso i Responsabili Esterni coinvolti;
   - verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD;
   - compilare o completare il Modello per la notificazione al Garante (***All. 1***) indicando esplicitamente se le azioni correttive previste sono già concluse od ancora *in itinere.*

c) nel caso risulti che la violazione possa comportare un elevato rischio per i diritti e le libertà degli interessati, fermo quanto previsto al punto precedente, il Referente privacy compila anche il Modello per la comunicazione della violazione agli interessati (vedasi ***All. 2***) e, in accordo con il RPD, individua le modalità più opportune con le quali effettuare tale comunicazione.

d) nelle ipotesi di cui ai precedenti punti b) e c), il Referente Privacy invia il verbale riportante gli esiti dell'analisi dei rischi sui diritti e le libertà delle persone fisiche, al SG, al quale spetta la decisione finale di procedere o meno alla notificazione all'Autorità Garante e se del caso alla comunicazione della violazione agli stessi Interessati. Il Segretario Generale deve riferire alla Giunta in merito al data breach occorso e alla gestione dello stesso.

NOTIFICAZIONE DEL DATA BREACH ALL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALII

Il Titolare del trattamento una volta venuto a conoscenza del data breach deve notificare l'accaduto all'Autorità Garante a mezzo di compilazione del Modello di cui all'***All. 1***, debitamente sottoscritto con firma digitale dal

Segretario Generale ed inviato nel più breve tempo possibile, **possibilmente entro 72 ore** dall'avvenuta conoscenza.

L'Ente in qualità del Titolare del trattamento deve considerarsi "a conoscenza" del *data breach* nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali trattati nell'ambito della propria attività.

Ove la notifica avvenga oltre tale limite temporale – in particolare, in caso di data breach particolarmente complesso e/o di serie di attacchi/violazioni consecutive che necessitano di una indagine complessa – è necessario dare conto delle ragioni / motivi che hanno comportato il ritardo.

Qualora non si disponga di tutte le informazioni previste dal format (*All.1*), è possibile inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni. 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 dei dati personali, l'Ente può chiedere all'Autorità Garante la cancellazione/revoca della notifica eseguita e l'incidente sarà registrato come un evento che non costituisce data breach.

Contestualmente alla notifica il Referente privacy aggiorna il "Registro dei Data Breach" (*All.3*)

COMUNICAZIONE DEL DATA BREACH AGLI INTERESSATI COINVOLTI

Nei casi in cui il Segretario Generale, valutato il verbale riassuntivo delle indagini svolte ricevuto dal Referente Privacy, riscontri la necessità di comunicare il data breach agli interessati in quanto la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, ne dà comunicazione al Referente Privacy.

Il Referente Privacy, successivamente:

- provvede a definire la comunicazione agli interessati che deve essere formulata con linguaggio chiaro e semplice e deve contenere tutti i seguenti elementi:
  - la natura della violazione dei dati personali;
  - le probabili conseguenze della violazione dei dati personali;
  - le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione;
  - il nome e i dati di contatto del responsabile della protezione dei dati.

- in accordo con RPD, definisce le modalità di comunicazione agli interessati:
  - invio della comunicazione a ciascun interessato, ove sia tecnicamente possibile reperirne i dati di contatto e l'attività possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec);
  - comunicazione pubblica / generalizzata (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc) ove non sia possibile identificare con precisione i singoli interessati coinvolti o non vi sia la disponibilità dei relativi dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati.

- Sottopone al SG, per l'approvazione definitiva, sia il testo che le modalità per la comunicazione individuati in accordo con RPD.

La comunicazione agli interessati deve essere formalizzata "senza ingiustificato ritardo".
Dell'avvenuta comunicazione è data informazione al RPD.

REGISTRAZIONE DELL'EVENTO – TENUTA DEL REGISTRO DEI DATA BREACH

Indipendentemente dalla notifica all'Autorità di controllo, il Titolare deve registrare e documentare qualunque violazione di dati personali (art. 33, par.5).

Il Titolare istituisce, quindi, un Registro dei data breach, a disposizione del Garante della privacy, e da fornire all'occorrenza in caso di accertamenti da parte dell'Autorità (***All. 3***). La conservazione e l'aggiornamento del Registro sono affidati al Referente Interno Privacy. Nel Registro devono essere riportate:

- le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate le violazioni;
- le conseguenze che le violazioni stesse hanno avuto;
- i provvedimenti adottati per porvi rimedio.

Nel Registro non devono essere riportati dati personali dei soggetti coinvolti nel data breach e nella gestione dello stesso.

Il Referente Interno Privacy dovrà aggiornare il Registro Data Breach contestualmente alla chiusura della fase di analisi, nel caso in cui risulti non necessaria la notifica al Garante Privacy o contestualmente all'invio di quest'ultima.

ATTIVITA' SUCCESSIVE

Se durante le fasi precedenti si sospetta che la violazione possa essere stata provocata in maniera intenzionale da un esterno o da un utente interno si attiva il processo di raccolta delle evidenze o prove con ulteriori investigazioni anche difensive.

L'attività, ove necessario, può essere gestita secondo quanto previsto dall'art. 391 *nonies*[1] o dall'art. 327 bis c.p.p.[2] e deve rispettare gli standard e le normative (raccolta e "catena di custodia") in termini di analisi forense, al fine di poter intraprendere successivamente un'azione legale nei confronti dell'eventuale responsabile.

Qualora non si riscontrasse questa condizione, l'analisi post-violazione sarà finalizzata all'apprendimento delle cause che hanno generato l'evento al fine di risolvere eventuali criticità collegate o ricorrenti.

Ad esito delle notificazioni al Garante ed agli interessati, il RPD deve:

- gestire in prima persona le relazioni e gli eventuali feedback pervenuti dal Garante e dalle altre Istituzioni coinvolte, coordinando – con l'ausilio della sua struttura di supporto – l'aggiornamento del "Registro dei Data Breach" (un cui modello è riportato nell'All. 3);
- gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente della Segreteria generale, ovvero dell'Ufficio legale o, ancora, dell'Area/Ufficio di riferimento interessata dalla la violazione.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, L'Ente svolge attività di informazione e formazione con riferimento ai contenuti del presente documento.

---

1 Se precedente all'instaurazione di un procedimento penale.

2 Se già instaurato il procedimento.

ALLEGATO 1 – MODELLO DI NOTIFICA AL GARANTE

Denominazione del Titolare del trattamento	
Dati di contatto	
Soggetto che effettua la notifica	
Ruolo del soggetto che effettua la notifica	
Responsabile della Protezione dei dati	
Dati di contatto del RPD	

Informazioni preliminari

Informazioni sulla notifica

☐ Nuova notifica
☐ Informazioni a completamento di una precedente notifica

Breve descrizione della violazione di dati personali

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

☐ Il _____
☐ Tra il _____ ed il _____
☐ In un tempo non ancora determinato
☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione di dati?

(Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
☐ Altro:

Dispositivo oggetto della violazione

☐ Computer
☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di un file
☐ Strumento di back-up
☐ Rete
☐ Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione e del numero approssimativo di record registrati

Interessati colpiti dalla violazione di dati

☐ N. _____ di persone fisiche
☐ Circa _____ persone fisiche
☐ Un numero (ancora) sconosciuto di persone
☐ Descrizione della/e categoria/e di interessati coinvolti:

(per la categoria di interessati, ad es.: dipendenti dell'Ente, utenti del servizio....., etc.)

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari
☐ Ancora sconosciuto
☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

(secondo le valutazioni del Titolare)

Contromisure (azioni preventive e correttive)

Misure tecniche e organizzative applicate prima della violazione

Misure tecniche e organizzative applicate successivamente alla violazione per attenuarne le conseguenze

Comunicazione agli interessati

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il _____

☐ No, perché:

Contenuto della comunicazione agli interessati

Canale utilizzato per la comunicazione agli interessati

ALLEGATO 2 – MODELLO DI COMUNICAZIONE ALL'INTERESSATO ( )

Denominazione del Titolare del trattamento	
Dati di contatto	
Soggetto che effettua la notifica	
Ruolo del soggetto che effettua la notifica	
Responsabile della Protezione dei dati	
Dati di contatto del RPD	

Interessato destinatario della comunicazione	

Modalità della comunicazione

☐ Raccomandata A/R
☐ PEC
☐ Posta elettronica
☐ Fax
☐ Altro: _____

Spett. Società/Egr. Sig...../

siamo spiacenti di informare che in data ..... abbiamo rilevato di aver subito una violazione dei dati personali la riguardano.

Nel prosieguo, in termini sintetici, è fornito – ai sensi di quanto previsto dall'art. 34 Regolamento UE n. 679/2016 (GDPR) – un quadro di quanto è accaduto.

La violazione è stata anche notificata al Garante.

Breve descrizione della violazione di dati personali e delle sue modalità

---

*

(*) Qualora la comunicazione richieda – ex art. 34, par. 3, lett. c) del GDPR – uno sforzo proporzionato (in relazione, per es. alle attività da svolgere e/o ai costi da sostenere), "(...) si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

Dispositivo oggetto della violazione

☐ Computer
☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di un file
☐ Strumento di back-up
☐ Rete
☐ Altro:

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari
☐ Ancora sconosciuto
☐ Altro:

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

Indicare:

A) Numero approssimativo di registrazioni dei dati personali oggetto della violazione
B) Categoria e numero approssimativo degli interessati coinvolti dalla violazione
C) Livello di gravità elevato della violazione per i diritti e le libertà delle persone fisiche
D) Possibili conseguenze della violazione.

(secondo le valutazioni del Titolare)

Misure tecniche e organizzative applicate preventivamente e quelle applicate successivamente alla violazione per porre rimedio alla violazione o per attenuarne le conseguenze

Per ulteriori informazioni, può essere contattato .....

ALLEGATO 3 – REGISTRO DEI DATA BREACH

DETTAGLI DELLA VIOLAZIONE	CONSEGUENZE DELLA VIOLAZIONE

[redacted]

Data evento e data conoscenza	Ufficio coinvolto	Natura dell'evento e breve descrizione della violazione	Tipologie di dati interessati	Categorie interessati coinvolti	Effetti accertati	Effetti ipotizzabili / possibili	Azioni correttive implementate	Azioni correttive da intraprendere	Notifica Garante	Comunicazione interessati	Doc. / allegati e/o email