Camera di Commercio
Salerno

DETERMINAZIONE SEGRETARIO GENERALE N.348 DEL 1 AGOSTO 2019

OGGETTO: APPROVAZIONE MODELLO GESTIONE INCIDENTI DI SICUREZZA (DATA BREACH).

IL SEGRETARIO GENERALE

Visto l'art. 66 del Regolamento per il personale camerale, approvato con D.I. 12.7.1982, relativo alle attribuzioni del Segretario generale;

Vista la legge 7 agosto 1990, n. 241 e smi;

Vista la legge 29 dicembre 1993, n. 580 e smi dal D.lgs.219/2016;

Visto il D. Lgs. 30 marzo 2001, n. 165 e smi;

Visto il DPR 2 novembre 2005, n. 254;

Visto il D.M. Del 7 febbraio 2013 con il quale il sottoscritto è stato nominato Segretario Generale dell'Ente Camerale;

Vista la deliberazione n. 20 del 19 febbraio 2013 con la quale la Giunta Camerale ha preso atto del predetto decreto ed approvato lo schema di contratto di lavoro del Segretario Generale dell'Ente.

Vista altresì la deliberazione n. 77 del 18 novembre 2016 , con la quale la Giunta camerale ha deciso di rinnovare, con decorrenza immediata, l'incarico del Segretario Generale

Vista la deliberazione n.12 del 6 marzo 2017 con la quale la Giunta camerale ha approvato l'assetto macro-organizzativo dell'Ente, così articolato:
I. Area "Affari generali e gestione risorse umane";
II. Area "Finanze"
III. Area " Anagrafe e patrimonio";
IV "Promozione economica - regolazione e tutela del mercato";

Vista la deliberazione n.9 del 13 settembre 2013, con la quale il Consiglio Camerale ha approvato il "Regolamento sull'ordinamento degli uffici e dei servizi ";

Vista la deliberazione della Giunta camerale n. 3 del 29 gennaio 2018 con la quale è stato approvato il "Piano delle Performance per gli anni 2018/2020";

Vista la deliberazione della Giunta camerale n. 2 del 29 gennaio 2018 con la quale è stato approvato il "Piano Triennale di Prevenzione della Corruzione per gli anni 2018/2020";

Vista la deliberazione del Consiglio Camerale n.13 del 17 dicembre 2018 con la quale è stato approvato il preventivo economico 2019;

Vista la deliberazione della Giunta camerale n. 82 del 17 dicembre 2018 con la quale sono stati approvati i budget direzionali ex art. 8 del DPR 254/05 per l'esercizio 2019;

Premesso che :

- il 25 maggio 2018 è entrato in vigore 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 (di seguito Regolamento) il quale ha abrogato la direttiva 95/46/CE (di seguito "RGPD");
- il RGPD detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni;
- le disposizioni del D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", nonché i provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata, ed è previsto comunque l'adeguamento della normativa nazionale alle disposizioni del Regolamento;
- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale;
- 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 per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità tenuto conto della specifica organizzazione dell'Ente;
- che il RGPD individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

  1. il 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;
  2. i Soggetti Delegati attuatori: attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati effettuati dall'Ente in esecuzione del Regolamento;
  3. il 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;
  4. il Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;

5. l'Incaricato autorizzato al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento;

Richiamata la propria determinazione n. 287 del 6 giugno 2018 con la quale, il Vice segretario Generale - Vicario - dott. Ciro Di Leva veniva designato Responsabile della Protezione dei dati personali (RPD) per la Camera di Commercio di Salerno;

Visto che il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;

Considerato che in esecuzione del GDPR ed al fine di attuare un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, è richiesto alle aziende e alle Pubbliche Amministrazioni di approntare un piano di protezione dei dati personali che, partendo dalla mappatura e dall'analisi dei trattamenti, effettui la valutazione del rischio di violazione ed individui infine le misure volte ad eliminare o almeno ridurre il rischio stesso;

Dato atto che permane comunque la possibilità che i dati personali vengano violati da parte di soggetti terzi, e che si rende quindi necessario prevedere una procedura da attuare nel caso si verificasse l'evento in questione.

Visto che l'articolo 4 del Regolamento UE 2016/679 (d'ora in poi GDPR) definisce "data breach" (o, nella traduzione italiana, 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 presso una Azienda o una Pubblica Amministrazione;

Visto, tra l'altro, che gli articoli 33 e 34 del GDPR si occupano rispettivamente di disciplinare la notifica di una violazione dei dati personali all'autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato;

Visto che la corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'organizzazione in caso di incidente e permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti;

Visto che l'art. 32 del Regolamento dispone che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali;

Considerato che, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH) predisposto dal dott. Ciro Di leva - Responsabile della protezione dei dati di concerto con il consulente per la privacy della società consortile " Infocamere" contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da

attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016;

Visti gli allegati allo schema di cui sopra, ed in particolare:
Allegato 1: violazione di dati personali - modello di comunicazione al garante;
Allegato 2: potenziale violazione di dati personali - modello di comunicazione al responsabile della protezione dei dati;

Ritenuto il predetto schema, con i relativi allegati, meritevole di approvazione perché il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui l'Ente deve notificare i data breach all'Autorità Garante ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre;

Visti i pareri espressi dal Capo Ufficio dell'Organizzazione, Sviluppo e Gestione Risorse Umane, dott.ssa Giovanna D'Auria e dal Capo Servizio AA.GG. e del Personale dott.ssa Emilia De Luca, in ordine alla solo legittimità dell'istruttoria e di tutti gli adempimenti procedurali e dal Dirigente d'Area I;

DETERMINA

di considerare la premessa narrativa presupposto di fatto e di diritto del presente provvedimento;

di approvare, lo schema di procedura per la gestione della violazione dei dati personali così come predisposto dal Responsabile della Protezione dei dati di concerto con il supporto per della società Consortile di Informatica delle Camere di Commercio Italiane - INFOCAMERE, che, allegato alla presente determinazione, ne forma parte integrante;

di dare atto che la succitata procedura contiene le indicazioni, le responsabilità e le azioni da attuare in caso di violazioni nel trattamento dei dati personali, con precipuo riferimento agli obblighi di notifica all'Autorità Garante per la protezione dei dati personali e di comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016, ivi compresi i relativi allegati "1" e "2";

di incaricare l'ufficio organizzazione, gestione e sviluppo risorse umane di assicurare la massima diffusione del presente provvedimento tra il personale dell'Ente incaricato del trattamento dei dati personali;

di pubblicare il documento sul sito istituzionale, alla Sezione: Amministrazione Trasparente/Altri contenuti/Trattamento dei dati personali e diramarlo al personale dipendente tramite disposizione interna.

Il presente documento informatico, firmato digitalmente ai sensi del Dlgs 82/2005 e smi, è esecutivo e sarà pubblicato nell'Albo camerale online, ai sensi dell'art. 32 della legge 18/6/09, n. 69.

Il Responsabile del Procedimento Amm.vo (dott.ssa Giovanna D'Auria)	Il Segretario Generale (Dott. Raffaele De Sio)

Atto sottoscritto con firma digitale ai sensi del D.Lgs. n. 82 del 07/03/2005 e s.m.i.

Camera di Commercio Industria Artigianato e Agricoltura di Salerno

SISTEMA DI GESTIONE DEI DATI PERSONALI

Procedura di gestione dei data breach

ai sensi del Regolamento UE 679/2016

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è descrivere le attività relative al processo di segnalazione e gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali in qualsiasi modalità svolti dalla Camera di Commercio di Salerno.

Tale processo regolamenta la gestione degli allarmi di sicurezza, la conduzione delle attività investigative funzionali alla individuazione di tutti gli elementi utili alla completa definizione di una violazione, l'attivazione delle strategie di contenimento o delle azioni correttive, la gestione degli adempimenti richiesti dalla normativa nei confronti del Garante per la protezione dei dati personali e degli interessati, le modalità per la tenuta di idonee registrazioni per documentare il rispetto degli obblighi imposti nel rispetto del principio di accountability.

Si tenga conto inoltre che:
a) nei rapporti di contitolarità ciascun contitolare attua la sua procedura per quanto attiene al trattamento dei dati che svolge. Nell'accordo di contitolarità possono tuttavia essere disposte specifiche procedure e/o modalità relativi ad obblighi di comunicazione tra le parti e tra queste ed il garante;
b) Per quanto attiene ai data breach relativi alle ipotesi in cui la Camera di commercio opera in qualità di responsabile esterno del trattamento, ex art. 28 del GDPR, dovranno essere osservate anche le indicazioni ed istruzioni fornite dal Titolare nel documento di nomina/designazione.

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 delle Aree/Uffici/Servizi della Camera di Commercio.

La presente procedura è diramata mediante Ordine di servizio del Segretario Generale ed è, altresì, consultabile in apposita sezione Intranet denominata "privacy".

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Notifica di una violazione dei dati personali all'autorità di controllo (art. 33 del GDPR)
2. Comunicazione di una violazione dei dati personali all'interessato (art. 34 del GDPR)
3. WP250rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottate il 03/10/2017 e riemesse il 06/02/2018

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	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)
RPD	Responsabile della protezione dei dati
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG	Segretario Generale della Camera di commercio

Evento	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi
Violazione (data breach)	Qualsiasi 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

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione
01/08/19	DETERMINAZIONE	SEGRETARIO GENERALE	N. 348

FASI DEL PROCESSO

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

RILEVAZIONE EVENTO E TRIAGE

La rilevazione di un evento 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: nell'ambito dell'attività di monitoraggio, assistenza e manutenzione da parte di fornitori esterni di applicativi, supporto sistemistico, servizi di consulenza, etc. ovvero da parte di utenti finali dei servizi della Camera di Commercio, ovvero da parte di Responsabili esterni nominati ex art. 28 del GDPR.
  In particolare, in tutti i contratti che attribuiscano funzioni di amministrazione di sistemi o deleghino trattamenti di dati personali a soggetti esterni qualificati o qualificabili come responsabili esterni del trattamento ex art. 28 GDPR, devono essere inserite clausole contrattuali che prevedono l'obbligo:
  - di comunicazione immediata di eventuali eventi di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse. Nello standard contrattuale è previsto che la segnalazione pervenga al Referente contrattuale;
  - di fornire, in caso di necessità, anche attraverso il RPD eventualmente nominato, la massima disponibilità e collaborazione per l'analisi e risoluzione di eventuali criticità emergenti per l'ambito di trattamento assegnato.

> Secondo il WP 29, il Regolamento "impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento, del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Inoltre, il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica". I sopra indicati sistemi di "segnalazione" dovrebbero, pertanto, essere predisposti (si pensi al SIEM) per indicare quando, con ragionevole certezza, si sia verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Le segnalazioni pervengono al Dirigente dell'Area di riferimento (o suo delegato) coinvolta dall'evento che attiva (anche in modalità videoconferenza) il team di primo intervento (TII) composto da:

- un referente CED ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente alla Camera di Commercio[1];
- un eventuale referente delle Società in house (o esterne) coinvolte nel trattamento[2];
- [il RPD].

Il team di primo intervento, sotto la responsabilità del citato Dirigente, ha il compito di verificare il perimetro dell'evento, ovvero almeno le seguenti informazioni:

1. sistema, infrastruttura, base dati oggetto dell'evento;

1Il termine "CED" indica, nella sua globalità, l'ufficio in cui opera l'Amministratore di sistema. L'"Amministratore di sistema" è la persona/e fisica/che (anche appartenenti a società designate Responsabili esterni del trattamento) debitamente incaricata dello svolgimento di detto ruolo, ai sensi della normativa vigente.

2A norma dell'art. 28, par. 3, lett. h) del GDPR, il Responsabile del trattamento "mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi... e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato".

2. tipologia dell'evento verificatosi;
3. tipologia e volume dei dati e degli interessati coinvolti:
4. misure di sicurezza applicate;
5. attività di remediation (azioni correttive) ipotizzabili.

In caso di mancato coinvolgimento di dati personali, il Team di primo intervento attribuisce le responsabilità per l'avvio delle eventuali azioni correttive e registra l'evento su una apposita scheda di rilevazione. Ad esito delle azioni correttive, la fase si chiude con il follow up di remediation.

Nel caso in cui l'evento coinvolga dai personali, viene attivata l'escalation che comporta la segnalazione della scheda di registrazione al RPD e la costituzione del Team di II intervento.

<u>Questa fase deve concludersi entro 24 ore dalla rilevazione dell'evento.</u>

Per una migliore chiarezza si riproducono alcune indicazioni del WP29.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.
2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".
3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.
4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione. Tuttavia, il titolare del trattamento potrebbe già disporre di una valutazione iniziale del rischio potenziale che potrebbe derivare da una violazione come parte di una valutazione d'impatto sulla protezione dei dati effettuata prima dello svolgimento del trattamento interessato. Tuttavia, tale valutazione può essere più generale rispetto alle circostanze specifiche di un'effettiva violazione e, pertanto, in ogni caso dovrà essere effettuata una valutazione aggiuntiva che tenga conto di tali circostanze.

ESCALATION, QUALIFICAZIONE DELLA VIOLAZIONE E REMEDIATION

Alla ricezione della scheda di segnalazione, il Dirigente dell'Area di riferimento costituisce il Team di secondo intervento (T2I) costituito da:

- il RPD della Camera di Commercio;
- il Responsabile dell'Ufficio/Capo Progetto/etc. responsabile del processo in relazione al quale si ipotizza la violazione di dati;
- un funzionario dell'Ente camerale in possesso di adeguate competenze di tipo giuridico;
- l'Amministratore di sistema ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente alla Camera;
- lo specialista della società o soggetto che ha realizzato/fornito il prodotto/servizio interessato dall'incidente e/o il RPD (ove nominato) o altro referente specializzato della Società in house coinvolta nel trattamento[3]
- l'eventuale ulteriore consulenza tecnica o giuridica qualora necessaria.

Il Team ha il compito di verificare, a norma dell'art. 33, par. 1, del GDPR, la probabilità che la violazione dei dati personali presenti un rischio (soprattutto se questo può qualificarsi come "elevato") per i diritti e le libertà delle persone fisiche e, di conseguenza, decidere le misure di risposta all'emergenza.
A tal fine:

a) sono raccolte o consolidate/approfondite le informazioni di cui al format per la comunicazione al Garante (All. 1), ove disponibili, anche al fine di minimizzare i tempi di risposta;
b) sono effettuate le seguenti valutazioni[4]:
   - natura della violazione e potenziale esposizione degli interessati (c.d. gravità dell'accadimento);
   - priorità, in funzione dell'urgenza (valutata sulla base di quanto velocemente potrebbero verificarsi danni);
   - impatto potenziale dell'esposizione degli interessati (valutazione dell'entità dei danni agli interessati)[5];
   - adeguatezza delle misure di sicurezza già implementate rispetto al potenziale danno arrecabile agli interessati.

Per un quadro delle valutazioni dei rischi si rinvia anche a quanto contenuto nelle Linee guida del WP29 (WP250rev.01).

Ad esito dell'analisi:

A. nel caso in cui la violazione – in funzione dell'adeguatezza delle misure implementate – non costituisca un rischio per gli interessati, il Dirigente o suo delegato provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD; copia del verbale deve essere inviato:
   - al RPD;
   - al SG, in qualità di designato del Titolare del trattamento per la condivisione finale sull'esito delle valutazioni nonché per consentire l'adozione delle necessarie disposizioni tese all'aggiornamento del "Registro dei Data Breach" come da format allegato (All. 4).

B. nel caso in cui sia stato valutato che le misure implementate siano insufficienti alla tutela degli interessati:
   1. il team provvede ad identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata ed il miglior esito ai fini della minimizzazione del possibile danno agli interessati
   2. il Dirigente provvede a:
      - definire ed assegnare responsabilità e tempistiche per la remediation, compresi i soggetti esterni coinvolti;
      - verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD;

3Cfr. nota n. 1

4Per la valutazione qualitativa degli impatti è possibile partire dai parametri di gravità/probabilità utilizzati nell'ambito dell'assessment dei trattamenti della Camera di commercio e dai valori ivi rilevati, procedendo per successivi affinamenti fino a focalizzare l'analisi sull'asset colpito dalla violazione.

5Ovvero danno fisico, materiale o immateriale, in particolare: perdita del controllo dei dati personali che li riguardano 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 significativo" cfr. considerando 75 e 85 GDPR.

- compilare o completare il Modello per la notificazione al Garante (All. 1) [6], indicando se le azioni correttive (c.d. attività di remediation) sono già concluse od ancora in itinere;
- inviare entrambi i documenti al SG (in qualità di delegato del Titolare del trattamento) per la condivisione finale sull'esito delle valutazioni e la decisione se procedere o meno alle notificazioni, nonché per consentire l'adozione delle necessarie disposizioni tese all'aggiornamento del "Registro dei Data Breach" come da format allegato (All. 4);
- predisporre, qualora ne ricorrano le condizioni, la comunicazione da inviare all'interessato (ovvero la comunicazione pubblica), contenenti le indicazioni riportate nell'All. 2.

Questa fase deve concludersi entro ulteriori 36 ore dalla rilevazione dell'evento.

INVIO DELLE NOTIFICAZIONI

Il Modello deve essere sottoscritto con firma digitale dal SG ed inviato formalmente al Garante nel più breve tempo possibile, entro 72 ore dall'avvenuta conoscenza da parte del Titolare, di un evento qualificabile come Data breach[7].
Ove avvenga oltre tale limite temporale è necessario corredarla dei motivi del ritardo[8].
Qualora non si disponga di tutte le informazioni previste dal format, è possibile inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni.
Il Dirigente dell'Area di riferimento invia il verbale ed il Modello sottoscritto dal SG:

- al RPD;
- al referente dell'Amministrazione Pubblica da cui eventualmente la Camera di Commercio ha ricevuto l'incarico di trattare i dati personali[9], previa valutazione di opportunità condotta congiuntamente con il SG ed a seguito dell'avvenuta notifica al Garante.

Ove le misure di cui al punto B) del paragrafo precedente siano adottate immediatamente, la fase si chiude con il follow up di remediation (mediante verbalizzazione degli esiti da parte del Dirigente dell'Area di riferimento)[10]
Nel caso in cui tali misure necessitino di maggior tempo per l'implementazione ovvero non siano in grado di minimizzare i rischi per gli interessati, il Dirigente dell'Area di riferimento:

a) provvede a definire i contenuti della comunicazione agli interessati, che – con linguaggio semplice e chiaro - deve contenere almeno 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.

   La comunicazione – un cui esempio è riportato nell'All. 2 – è sottoposta a parere del RPD e ad approvazione del SG.

b) verifica la fattibilità di reperimento dei dati di contatto degli interessati coinvolti o potenzialmente coinvolti; nel caso in cui si valuti che la comunicazione agli interessati possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec), provvede all'invio massivo della comunicazione.

c) Ove non vi sia disponibilità di dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati, provvede a darne pubblicità nelle modalità concordate con SG e RPD (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc.).

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

6Il Modello – in attesa della revisione da parte del Garante - è tratto dall'Allegato al provvedimento del Garante n. 392 del 2/07/2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche".
7Nelle fasi indicate in precedenza sono disponibili 12 ore che possono essere distribuite come si ritenga maggiormente opportuno.
8ad es., data breach particolarmente complesso, serie di attacchi/violazioni consecutive che necessitano di una reazione complessa.
9Ad es., sulla base di una convenzione/protocollo d'intesa.
10"Non è richiesta la comunicazione all'interessato... se 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" (art. 34, par. 3, lett. b del GDPR).

E' bene ricordare che:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

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 al fine di valutare la sussistenza delle condizione per una segnalazione all'Autorità giudiziaria.
Al termine della fase di gestione dell'emergenza, si procederà con l'analisi di post violazione finalizzata all'apprendimento delle cause che hanno generato l'evento e allo scopo di eliminare o minimizzare le criticità emerse.
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, verificando l'aggiornamento del "Registro del Data Breach" (un cui modello è riportato nell'All. 4);
- deve gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente della Segreteria generale, ovvero 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.

MATRICE DELLE RESPONSABILITA'

Legenda

- R = Responsabile
- C = Coinvolto
- I = Informato

Fase	*Attività*	Dirigente dell'Area coinvolta	Segretario Generale	Responsabile della Protezione dei Dati	Funzionario con competenze legali	CED / Amministratore di sistema	Società esterne Responsabili del trattamento	
	Soggetto/ Struttura							
RILEVAZIONE E TRIAGE	Rilevazione evento	R				C	C	
	Triage	R				R	R	
	Escalation	R		I	I	I	I	
QUALIFICAZIONE	Raccolta informazioni	R		C	C	C	C	
	Valutazione d'impatto	R		C	C	C	C	
	Verbalizzazione esiti	R	I	I				
	Tracciamento su Registro Data Breach		R	I				
	Identificazione azioni correttive	R		C		C	C	
	Implementazione azioni correttive	R				R	R	
	Compilazione format notifica	R		C				
	Monitoraggio azioni correttive	R		C		C	C	
NOTIFICAZIONI	Sottoscrizione ed invio format notifica	I	R	C				
	Informativa a PA partner	R	I					
	Predisposizione comunicazione Interessati	R	C	C				
	Approvazione comunicazione		R	C				
	Invio o pubblicazione comunicazione	R	I	I				
	Avvio indagini difensive	R	C	I	C			

Legenda

- R = Responsabile
- C = Coinvolto
- I = Informato

Fase	*Attività*	*Soggetto/ Struttura*: Dirigente dell'Area coinvolta	Segretario Generale	Responsabile della Protezione dei Dati	Funzionario con competenze legali	CED / Amministratore di sistema	Società esterne Responsabili del trattamento	
ATTIVITÀ SUCCESSIVE	Rapporti con il Garante	I	C	R				
	Rapporti con interessati	R	I	C				

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?

☐ Si, 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 – CONTATTI DI EMERGENZA DEI SOGGETTI COINVOLTI NELLA PROCEDURA

RPD	
CED/Amministratore di sistema	
HELP DESK INFOCAMERE	
ALTRO	

ALLEGATO A – REGISTRO DEI DATA BREACH

N. record/anno	Banca dati/Archivio coinvolto dalla violazione	Processo/progetto ed Ufficio di riferimento	Cause della violazione (vulnerabilità)	Tipologia e modalità di realizzazione	Conseguenze della violazione	Azioni correttive adottate	Follow up azioni correttive	Notifica al Garante (si/no) [indicare protocollo comunicazione]	Notifica agli Interessati (si/no) [indicare protocollo comunicazione]	Prescrizioni specifiche del Garante